TECHNICAL UNIVERSITY OF CRETE
ELECTRICAL AND COMPUTER ENGINEERING DEPARTMENT
TELECOMMUNICATIONS DIVISION

Backscattering Ambient Signals: Assisting Radios & Tracking Planes

by

Iosif Vardakis

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DIPLOMA OF

MASTER OF SCIENCE IN ELECTRICAL AND COMPUTER ENGINEERING

October 2022

THESIS COMMITTEE

Professor Aggelos Bletsas, *Thesis Supervisor*
Professor George N. Karystinos
Professor Michalis E. Zervakis

Table of Contents

List of Figures

Abstract

This work's main objective was to exploit ambient signal backscattering to aid radio communication, through a smart reflective surface or detect airplane reflections through a passive radar system.

First, ultra-low cost, commodity, radio frequency identification (RFID) tags are utilized as elements of a reconfigurable intelligent surface (RIS). Such batteryless tags are powered and controlled by a software-defined radio (SDR) reader, with properly modified software, so that a source-destination link is assisted, operating at a different band. Signal model includes small-scale and large-scale fading, direct link, as well as specific parameters relevant to reflection (i.e., backscatter) radio, such as antenna structural mode and reflection efficiency, typically overlooked in the literature. An algorithm is offered that computes the optimal RIS configuration with complexity of $\mathcal{O}(M \log M)$ in number of elements M, instead of intractable exponential complexity of exhaustive search, while accommodating any number $K \geq 2$ of loads. With the proposed algorithm, it is shown that performance gains reach a plateau for constant element spacing and increasing number of elements, suggesting that the weak, passive nature of backscattered links limits the performance gains, even with perfect channel estimation. A concrete way is offered to design and prototype a wireless, batteryless, RF-powered, reconfigurable surface and a proof-of-concept is experimentally demonstrated.

Then, an FM passive radar station capable of tracking airplanes in Cartesian 3D coordinates was developed. The station was constructed using a low-cost SDR, based on the LimeSDR USB platform; the latter is a relatively low-cost SDR, in the order of 300$. The station is complemented with a 5-element Yagi antenna for observation and another 3-element Yagi antenna, for observing the FM radio broadcasting stations. Signals from different FM broadcasting stations were collected and amplitude-range-Doppler(ARD) plots were created. Then, a bistatic tracker was designed for each broadcasting station, estimating the bistatic range and Doppler shift from each ARD plot. Finally, the estimated range-Doppler frequency shift pairs from each station were fed as input to the Cartesian tracker, which was designed to offer 3D tracking. Simulation results showed an error below 100m in each direction. The system exploits

space diversity, due to the multiple spatially separated broadcasting stations required as input, and frequency diversity, due to processing of multiple frequency bands of interest. The system is scalable, since increasing the number of broadcasting stations utilized requires no change in the processing chain. Experimental results with the low-cost LimeSDR platform corroborate theoretical findings and demonstrate the utility of this work, as a testbed for further research and development.

Acknowledgements

First of all, I would like to thank my supervisor Prof. Aggelos Bletsas for giving me the opportunity to work on such an exciting topic and for all his invaluable support throughout this thesis.

I am extremely grateful to my friends and colleagues Dr Georgios Vougioukas, Spyridon Peppas, Georgios Kotridis, Konstantinos Skyvalakis, Evangelos Giannelos and Manos Andrianakis for the fun time and cooperation in the Telecom Lab.

Of course, I would like to acknowledge and respect the priceless support provided by my family throughout my studies.

Additionally, I'm extremely grateful to Dr. Vougioukas for hearing and discussing my (many) questions, while also, for his tremendous help with the experimental setup.

Last but not least, Roza thank you for all the love and support throughout these years.

The research work was supported by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the "First Call for H.F.R.I. Research Projects to support Faculty members and Researchers and the Procurement of High-cost research equipment" (Project Number: 2846).

Chapter 1

Introduction

Significant interest has been attracted recently on reconfigurable intelligent surfaces (RISs), which are viewed as a way to control the environment, with a large number of passive elements, i.e., without amplification; such surfaces are envisioned to offer a *focusing* effect (e.g., review work in [2], [3], and references therein). Despite the fact that RIS is a special case of bistatic backscatter radio [4–6], or multistatic scatter radio [7], [8], such connection is not widely known in the literature. Backscatter, i.e., *reflection* radio has been extensively used in radio frequency identification (RFID) and recently was proposed for sensor networking applications (e.g., work in [9] for monostatic interrogation and work in [10–16] for bistatic, batteryless sensor interrogation and references therein). Review material and connection to ambient backscatter communication [17], a special case of bistatic backscatter, can be found in [18] and references therein.

Another technology that exploits ambient signal's reflections on objects is passive bistatic radar (PBR). This type of radar operates in a bistatic manner [19], using non-cooperative illuminators of opportunity (IoO), such as FM radio [20] or DTV stations to detect targets [21]. Therefore, expensive radar transmitters and licensing is not needed and pre-existing signals are used, without exacerbating the spectral congestion. Instead, PBR station operates with cheap components such as off-the-shelf software-defined radio (SDR) receivers, with prices starting at 8$ (RTLSDR), accompanied with a standard personal computer [22]. Other characteristics include fast update rates (i.e $0.1 - 1$ s) [20] and covert operation, since there are no energy emissions from the PBR station, in contrast to an active radar system. Moreover, although the narrow bandwidth leads to low range and bearing accuracy, the large integration times leads to an excellent Doppler resolution.

PBR is known for its prominent use in countering stealth technology [23]. Stealth targets are mainly designed to either absorb or scatter the electromagnetic wave in an angle that differs from the incident to prevent detection by a monostatic radar. PBR use could be beneficial in detecting stealth aircraft. This is due to the bistatic nature of the PBR and the characteristics of the VHF (i.e. FM) or the UHF (i.e. DVB-T). The wavelength of these frequencies is in the order of meters, where the

aircraft absorption capability is considered not as strong as in the microwave region. Also, the utilization of GPS signals have enabled multistatic PBR operation [24].

Also, there are strong links between tag ambient backscattering tags and PBR, demonstrated in [25], where an increase of communication range using PBR techniques and DTV signals was demonstrated both theoretically and experimentally; experimental results showed a possible rate of 1 kbps at a range of 100 meters.

1.1 Related Studies

According to [26], a near-field, squared-shaped RIS can offer limited gains. Firstly, given a large surface, the distance between the source and the elements of RIS can be much greater than the link distance (i.e. distance from source to the center of RIS), resulting in significant attenuation. Secondly, distant elements of the surface exhibit lower local effective areas. Finally, the polarization mismatch increases for the elements deployed far away from the center of the surface. Similarly, authors in [27], pinpoint that the received power scattered by a RIS is bounded as the size of the surface increases.

Assuming the presence of a RIS, work in [28] considered the joint maximization of spectral and energy efficiency in a multi-user MISO downlink network; alternative optimization of base station beamforming and RIS phase shifts was employed, subject to individual link budget guarantees for the mobile users. Such formulation led to non-convex optimization problems, addressed by two computationally affordable methods. In order to make the problem more tractable, the authors assumed infinite-resolution phase shifters, no direct links and perfect channel state information (CSI) available at the base station; comparison to multi-antenna amplify-and-forward relaying was also performed. In [29], the performance of a single-cell multiuser system aided by multiple RISs was evaluated. Through simulations, it was shown that the RIS-aided system can outperform full-duplex relaying, in terms of spatial throughput, when the number of RIS elements exceeds a certain value. Differently from the single-user case where the RIS should be deployed near the BS or user for rate maximization, RISs (in the multi-user system) should be distributed across the whole network.

Work in [30] introduced expressions to compute the power reflected from a RIS as a function of distance between the transmitter or receiver and the RIS, the size of the RIS and the phase transformation applied by RIS. Calculations were based on the general scalar theory of diffraction and the Huygens-Fresnel principle. Free space path loss models were offered in [31], along with an experimental testbed for their

verification. It is noted that a significant issue on RIS implementation is the mutual coupling. Conceptually, each element modifies the phase of the impinging EM wave. When the elements are spaced by at least half of the wavelength, mutual coupling among them is usually ignored and each element can be designed independently of the others [32].

Work in [33] employed tools from stochastic geometry and studied the effect of large-scale deployment of RISs on the performance of cellular networks. Direct links assumed blocked and blockages, such as buildings or trees, were modeled with a line Boolean model. A subset of the blockages was equipped with RISs and a performance study on cellular networks was performed, assuming no inter-cell interference and small-scale fading effect.

Joint study of RIS with non-orthogonal multiple access (NOMA) has been recently an attractive research topic [34–37]. There exist two dominant NOMA schemes: the first is relevant to power domain multiplexing, which assumes that different users are allocated different transmission power, based on their channel conditions; the second is relevant to code domain multiplexing, which assumes that different users are assigned different codes, multiplexed over the same time-frequency resources. Complexity of successive interference cancellation (SIC) in both schemes was studied.

Work in [38–42] proposed metasurfaces in order to manipulate electromagnetic (EM) waves, allowing for anomalous reflection, full EM absorption, refraction, and polarization control. In [38], [41], [42] an application programming interface (API) is envisioned to exist on a server, in order to control the metasurfaces. Evaluations, solely based on simulations, showed improved received power and coverage.

A small number of experimental testbeds has recently emerged, e.g., work in [1,43–45]; [43] offered a 36-element array, with phase shifters helping endpoints whose line-of-sight (LoS) is blocked; [44] developed a RIS with 256 elements exploiting positive intrinsic-negative (PIN) diodes for $2-$bit phase shifting; [1] utilized software-controlled, 2-load RF switches in groups, in order to select different surface configurations with thousands of elements, exploiting feedback from the destination; a RIS-based system was implemented in [45] with 256 elements (controlled with varactor diodes), which could facilitate amplitude-and-phase-varying modulation, assisting 2×2 MIMO transmission. In principle, each element should be controlled by a dedicated digital-to-analog converter (DAC). Due to hardware limitations however, two DACs were used in order to control the elements. The distance between the RIS and the two receiving antennas was about 1.5 meters and cables were required to control the RIS elements from a dedicated field programmable gate array (FPGA). All offered

testbeds so far are based on wired prototypes.

Prior art in PBR [20] has shown that it is possible to localize and track targets in 3D, using range and bearing measurements. However the accuracy was limited by the low accuracy of the bearing measurements. In [46], a combination of multilateration techniques, along with an array of antennas as a direction finder, demonstrated a target accuracy of 250 m at a range of 20 km from the receiver. Authors in [47] demonstrate in both theory and simulation results, the significant performance improvement in terms of position and velocity estimation of a PBR that uses an increasing number of antennas.

Localization algorithms have been proposed for the single-receiver and multiple transmitter case or vice versa, such as in [48], where two closed-form solutions are derived. For the multiple-receiver to multiple-transmitters case, [49] uses a closed-form two-step weighted least squares (WLS) method, to minimize the weighted equation error energy and estimate the target's state.

In [50], experimental investigation showed that increasing the number of PBR receivers, in both FM and DVB-T bands, is beneficial in terms of the detection range, localization error and tracking quality. This improvement occurs due to the increased number of bistatic geometries, exploitation of complementarities in the FM and DVB-T waveforms and observation of the target from various aspect angles (multistatism).

In [51], PBR target detection is improved using a combination of multiple FM channels, exploiting frequency diversity. As a result, performance deterioration due to instantaneous bandwidth variations of FM channels is reduced significantly. In [52], a supersonic rocket was launched and tracked in 3D Cartesian coordinates with DVB-T PBR. This work demonstrated the ability of a PBR to track targets, whose position and velocity changes rapidly, due to the high refresh rate.

Finally, various projects over the last few years have offered open-source software, helping researchers and enthusiasts in learning and extending PBR technology [53], [54].

1.2 Contribution

This work exploits commodity, ultra-low cost, commercial radio frequency identification tags *as the RIS elements*. Such batteryless tags are powered and controlled by a software-defined radio (SDR) reader, operating at carrier frequency f_2, with properly modified software, so that a source-destination link, operating at a *different* carrier

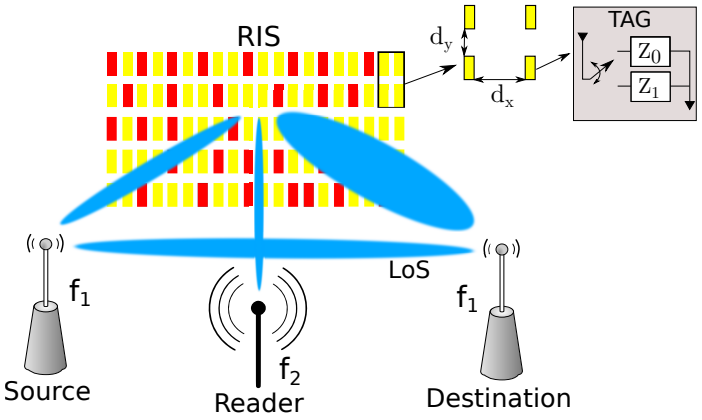


Figure 1.1: The proposed wireless surface with commodity, wirelessly-controlled, RF-powered, RFID tags.

frequency f_1, is assisted (Fig. 1.1).

It is found for the first time in the literature (to the best of our knowledge): a) the optimal gain and corresponding best RIS element configuration, with tractable polynomial complexity (instead of exponential) in number of elements and b) the way to design and prototype a wireless, batteryless, RF-powered RIS, with commodity RFID tags. Future extensions at various carrier frequencies could be accommodated, through simple modifications in the antenna and matching network of each RFID tag, as well as modifications in the RFID protocol for efficient, RIS-tailored operation. The contributions are summarized as follows:

- Signal model includes small-scale and large-scale fading, as well as specific parameters relevant to reflection (i.e., backscatter) radio, such as antenna structural mode and reflection efficiency, typically overlooked in the literature; such modeling is critical in RIS-relevant research, due to the lack of amplification, the passive nature of reflecting elements and thus, the inherently weak signals involved.

- An algorithm that computes the optimal RIS configuration with tractable polynomial complexity of $\mathcal{O}(M \log M)$, instead of intractable complexity of K^M for exhaustive search with large M, where $K \geq 2$ is the number of loads per RIS element and M is the total number of RIS elements. The algorithm can accommodate *any* set of reflection coefficients (e.g., not necessarily of common amplitude). Such algorithm allows for careful communication theory studies when M is in the order of thousands.

- Using the proposed optimization method, it is numerically demonstrated that

performance gain will reach a plateau if RIS element spacing is kept constant, for increasing number of elements in the order of thousands. This finding corroborates recent reports on bounded RIS performance and suggests that even with perfect channel estimation, the weak nature of backscattered links limits the performance gains, even for large number of RIS elements. Numerical results also suggest that amplification may be needed in practical setups.

- A RIS prototype is demonstrated, which is completely wireless and batteryless, using commercial (Gen2) RFID tags as the RIS elements. The surface is controlled by a software-defined radio reader, running a carefully modified stack of the Gen2 RFID protocol. Experimental results offer, to the best of our knowledge, the first wireless, batteryless RIS and future modifications and enhancements are also proposed.

- A PBR station has been developed using low-cost hardware, including two FM antennas, a relatively low-cost SDR (300$) and a standard laptop. The stages of signal processing are presented and discussed. Experimental results are offered in the bistatic coordinates, where a Kalman filter-based bistatic tracker is used to estimate the target's state, evaluating the PBR's performance. Spatial and frequency diversity is examined in a multistatic PBR setup, using a scalable two-stage Cartesian 3D tracker and its performance has been validated through simulations. The fully-operational PBR station, developed in this work, provides a testbed for further research and development.

1.3 Organization

The rest of the work is organized as follows: Chapter 2 offers a detailed system and signal model, tailored to the weak nature of backscattered signals along with the algorithm that can compute the optimal RIS configuration, given CSI, with tractable complexity; Chapter 3 describes the batteryless, wireless RIS implementation; Chapter 4 offers evaluation, both in terms of simulations, as well as experimental results. Chapter 5 provides basic PBR theory, the system model and the signal processing chain, including clutter removal, correlation processing and detection; Chapter 6 presents a target tracker operating in the bistatic coordinates, i.e., estimation of range and Doppler frequency pair for a given illuminating transmitter, accompanied with experimental results. Chapter 7 offers a cartesian 3D tracker that uses the bistatic tracks' range-Doppler frequency pairs from at least three illuminating transmitter-

receiver pairs, to obtain a 3D position and velocity estimate of the target's state. Finally, conclusions and future work are offered in Chapter 8.

Notation: $\mathbf{0}_N$ denotes the all-zeros vector; the phase of complex number z is denoted as $\angle z$, while $\Re\{z\}$ denotes the real part of z; the distribution of a proper complex Gaussian $N \times 1$ vector $\boldsymbol{x}$ with mean $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$ is denoted by $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma}) \triangleq \frac{1}{\pi^N \det(\Sigma)} \mathrm{e}^{-(\boldsymbol{x}-\boldsymbol{\mu})^H \boldsymbol{\Sigma}^{-1}(\boldsymbol{x}-\boldsymbol{\mu})}$; the special case of a circularly symmetric complex Gaussian $N \times 1$ vector corresponds by definition to $\mathcal{CN}(\mathbf{0}_N, \boldsymbol{\Sigma})$; expectation of function $\mathrm{g}(\cdot)$ of random variable x is denoted by $\mathbb{E}[\mathrm{g}(x)]$; the derivative of a variable x is denoted by $\dot{x}$.

Chapter 2

Optimal RIS configuration

2.1 Channel Model

A source-destination link is assisted by an array of M tags/RIS elements. The following *large-scale* channel path-loss model is adopted [55]:

$$\mathsf{L}_{\mathrm{X}} \propto \left(\frac{\lambda}{4\pi d_0^{\mathrm{X}}}\right)^2 \left(\frac{d_0^{\mathrm{X}}}{d_{\mathrm{X}}}\right)^{v_{\mathrm{X}}}, \tag{2.1}$$

where $\mathrm{X} \in \{\mathrm{SD}, \mathrm{ST}_m, \mathrm{T}_m\mathrm{D}\}$ denotes the source-to-destination, source-to-tag m and tag m-to-destination, respectively; λ is the carrier wavelength, d_0^{X} is a reference distance, v_{X} is the path-loss exponent and d_{X} is the distance for link X.

Flat fading is assumed; complex channel coefficients h_{SD}, h_{ST_m} and $h_{\mathrm{T}_m\mathrm{D}}$ denote the baseband channel coefficients for the source-destination, source-tag and tag-reader link, respectively. Due to strong line-of-sight (LoS) signals present in the problem, *small-scale* Rice flat fading channel model [55] is mainly adopted:[1]

$$h_{\mathrm{T}_m\mathrm{D}} \sim \mathcal{CN}\left(\sqrt{\frac{\kappa_{\mathrm{T}_m\mathrm{D}}}{\kappa_{\mathrm{T}_m\mathrm{D}}+1}}\,\sigma_{\mathrm{T}_m\mathrm{D}}, \frac{\sigma^2_{\mathrm{T}_m\mathrm{D}}}{\kappa_{\mathrm{T}_m\mathrm{D}}+1}\right), \tag{2.2}$$

where $h_{\mathrm{T}_m\mathrm{D}} \triangleq |h_{\mathrm{T}_m\mathrm{D}}|\, e^{-j\phi_{\mathrm{T}_m\mathrm{D}}}$, $k_{\mathrm{T}_m\mathrm{D}}$ is the power ratio between the deterministic LoS component and the scattering components and $\mathbb{E}[|h_{\mathrm{T}_m\mathrm{D}}|^2] = \sigma^2_{h_{\mathrm{T}_m\mathrm{D}}}$ is the average power of the scattering components. For link budget normalization purposes, $\sigma^2_{h_{\mathrm{T}_m\mathrm{D}}} = 1$ will be also assumed (other values could be easily accommodated into the large-scale, average coefficients). Similar notation and assumptions hold for h_{ST_m}, $m \in \{1, 2, \ldots, M\}$ and h_{SD}. It is noted that for $\kappa = 0$, Rice is simplified to Rayleigh fading.

Quasi-static block fading is assumed, i.e., the channel remains constant for L_c (source-destination link) symbols and changes independently between channel coherence time periods. Channel coefficients h_{SD}, $\{h_{\mathrm{ST}_m}\}$, $\{h_{\mathrm{T}_m\mathrm{D}}\}$, $m \in \{1, 2, \ldots, M\}$ are

[1] The complex channel is the superposition of $\sqrt{\frac{\kappa_{\mathrm{T}_m\mathrm{D}}}{\kappa_{\mathrm{T}_m\mathrm{D}}+1}}\,\sigma_{\mathrm{T}_m\mathrm{D}}\, e^{j\theta} + \mathcal{CN}\left(0, \frac{\sigma^2_{\mathrm{T}_m\mathrm{D}}}{\kappa_{\mathrm{T}_m\mathrm{D}}+1}\right)$ with random θ.

assumed independent in the numerical results. Furthermore, the following notation is also adopted:

$$h_m = h_{\mathrm{ST}_m}\, h_{\mathrm{T}_m\mathrm{D}} = |h_{\mathrm{ST}_m}\, h_{\mathrm{T}_m\mathrm{D}}|\, e^{-j\phi_m}, m \in \{1, 2, \ldots, M\},$$
$$h_0 = h_{\mathrm{SD}}, m = 0. \tag{2.3}$$

2.2 Signal Model

The baseband source message $c(t)$ is given by:

$$c(t) = \sqrt{2P}\, m(t) \tag{2.4}$$

where $\mathbb{E}[|m(t)|^2] = 1$. Different normalization could be incorporated into the large-scale coefficients. The baseband complex equivalent of the scattered waveform from tag m follows [6]:

$$u_m(t) = \sqrt{\eta\, \mathsf{L}_{\mathrm{ST}_m}}\, [A_s - \Gamma_m(t)]\, h_{\mathrm{ST}_m}\, c(t), \tag{2.5}$$
$$\Gamma_m(t) \in \{\Gamma_1, \Gamma_2, \ldots, \Gamma_K\}, \tag{2.6}$$

where $\Gamma_m(t)$ stands for the modified (complex) reflection coefficient for tag m, assuming that the tag can terminate its antenna between K loads and η models the (limited) tag power scattering efficiency. It is noted that for passive (amplification-free) tags, $|\Gamma_k| \leq 1$, while for commercial RFID tags, $K = 2$. Parameter A_s stands for the load-independent *structural mode* that solely depends on tag's antenna [56], commonly overlooked in the literature; $A_s = 1$ only for *minimum scattering* antennas, i.e., antennas that do not reflect anything when terminated at open (i.e., infinite) load, corresponding to unit reflection coefficient (and in that case $A_s - \Gamma = 0$).

The received demodulated complex baseband signal at the destination is given by the superposition of the source and all tags' backscattered signals propagated through

wireless channels h_{SD} and $\{h_{\mathrm{T}_m\mathrm{D}}\}$, respectively:

$$\begin{aligned} y(t) &= \sqrt{\mathsf{L}_{\mathrm{SD}}}\, h_{\mathrm{SD}}\, c(t) + \sum_{m=1}^{M} \sqrt{\mathsf{L}_{\mathrm{T}_m\mathrm{D}}}\, h_{\mathrm{T}_m\mathrm{D}}\, u_m(t) + n(t) \\ &= \sqrt{\mathsf{L}_{\mathrm{SD}}}\, h_{\mathrm{SD}}\, c(t) + n(t) \\ &\quad + \sum_{m=1}^{M} \sqrt{\eta\, \mathsf{L}_{\mathrm{ST}_m} \mathsf{L}_{\mathrm{T}_m\mathrm{D}}}\, h_{\mathrm{ST}_m}\, h_{\mathrm{T}_m\mathrm{D}}\, \left[A_s - \Gamma_m(t)\right]\, c(t) \\ &= \sqrt{2P} \left[\sqrt{g_0}\, h_0 + \sum_{m=1}^{M} \sqrt{g_m}\, h_m\, \mathcal{Y}_m(t) \right] m(t) + n(t), \end{aligned} \tag{2.7}$$

where $n(t)$ is the thermal noise at the receiver and

$$g_0 = \mathsf{L}_{\mathrm{SD}}, \tag{2.8}$$

$$g_m = \eta\, \mathsf{L}_{\mathrm{ST}_m} \mathsf{L}_{\mathrm{T}_m\mathrm{D}}\, \mathbb{E}\left[\left|A_s - \Gamma_m(t)\right|^2\right], \tag{2.9}$$

$$\mathcal{Y}_m(t) = \frac{A_s - \Gamma_m(t)}{\sqrt{\mathbb{E}\left[\left|A_s - \Gamma_m(t)\right|^2\right]}}, \tag{2.10}$$

$$y_m\left[\Gamma_m(t)\right] \triangleq \sqrt{g_m}\, h_m\, \mathcal{Y}_m(t). \tag{2.11}$$

Notice that $\mathbb{E}[|h_0|^2] = \mathbb{E}[|h_m|^2] = \mathbb{E}[|\mathcal{Y}_m|^2] = 1$ since $\mathbb{E}[|h_m|^2] = \mathbb{E}[|h_{\mathrm{ST}_m}|^2]\,\mathbb{E}[|h_{\mathrm{T}_m\mathrm{D}}|^2]$, due to the followed assumptions. It is also noted that $\mathbb{E}\left[\left|A_s - \Gamma_m(t)\right|^2\right] = (1/K)\sum_{k=1}^{K} \left|A_s - \Gamma_k\right|^2$.

The above model is valid when coupling among the tags is negligible, i.e., the tags are separated by distance at least equal to $\lambda/2$. Additive thermal noise $n(t)$ is modelled by a complex, circularly symmetric, additive Gaussian noise process with $\mathbb{E}[|n(t)|^2] = N_0 B$, where B stands for receiver's bandwidth.[2]

RIS targets at SNR improvement, by controlling the environment, through proper selection of the reflection coefficient at each element. According to Eq. (2.7), the

[2] $N_0 = k_b T_\theta$, where k_b and T_θ are the Boltzmann constant and receiver temperature, respectively.

following instantaneous power maximization problem is formulated:

$$\max_{\{\mathcal{Y}_m(t)\}} \left| \sqrt{g_0}\, h_0 + \sum_{m=1}^{M} \sqrt{g_m}\, h_m\, \mathcal{Y}_m(t) \right|^2 2P \tag{2.12}$$

$$\Leftrightarrow \max_{\{\mathcal{Y}_m(t)\}} \left| \underbrace{\sqrt{g_0}\, h_0}_{y_0} + \sum_{m=1}^{M} \sqrt{g_m}\, h_m\, \mathcal{Y}_m(t) \right| \tag{2.13}$$

$$= \max_{\{\Gamma_m(t)\}} \left| y_0 + \sum_{m=1}^{M} y_m \left[\Gamma_{m(t)}\right] \right|, \tag{2.14}$$

which cannot be solved with exhaustive search, since each RIS element (among M elements) can select among K loads, i.e., $\Gamma_m(t) \in \{\Gamma_1, \Gamma_2, \ldots, \Gamma_K\}$, and thus, there are K^M possible load configurations. Even for $K = 2$ and $M = 100$, exhaustive search among 2^{100} load configurations is not an option.

The following offers an *optimal* method for the above optimization problem, with log-linear complexity $\mathcal{O}(M \log(M))$ in the number M of RIS elements, instead of the exponential (in M) complexity of exhaustive search.

The problem above is similar to noncoherent sequence detection of orthogonally-modulated sequences, solved with polynomial complexity in [57]. The trick is to introduce an auxiliary scalar variable ϕ into the problem of Eq. (2.14):

$$\begin{aligned} &\max_{\{\Gamma_m(t)\}} \max_{\phi\in[0,2\pi)} \Re\left\{ e^{-j\phi} \left(y_0 + \sum_{m=1}^{M} y_m \left[\Gamma_{m(t)}\right] \right) \right\} = \\ &\max_{\phi\in[0,2\pi)} \max_{\{\Gamma_m(t)\}} \left(\Re\left\{ e^{-j\phi} y_0 \right\} + \sum_{m=1}^{M} \Re\left\{ e^{-j\phi} y_m \left[\Gamma_{m(t)}\right] \right\} \right) \end{aligned} \tag{2.15}$$

2.3 $K = 2$ Loads

For a given point $\phi \in [0, 2\pi)$, the innermost maximization in Eq. (2.15) is separable for each $\Gamma_m(t)$ and hence, splits into independent maximizations for any $m = 1, 2, \ldots, M$:

$$\begin{aligned}
\hat{\Gamma}_m(t) &= \underset{\Gamma_m(t)\in\{\Gamma_1,\Gamma_2\}}{\arg\max}\ \Re\left\{\mathrm{e}^{-j\phi} y_m\left[\Gamma_m(t)\right]\right\} \\
&\Leftrightarrow \Re\left\{\mathrm{e}^{-j\phi} y_m\left[\Gamma_1\right]\right\} \underset{\hat{\Gamma}_m(t)=\Gamma_2}{\overset{\hat{\Gamma}_m(t)=\Gamma_1}{\gtrless}} \Re\left\{\mathrm{e}^{-j\phi} y_m\left[\Gamma_2\right]\right\} \\
&\Leftrightarrow \Re\left\{\mathrm{e}^{-j\phi}\left(y_m\left[\Gamma_1\right] - y_m\left[\Gamma_2\right]\right)\right\} \underset{\hat{\Gamma}_m(t)=\Gamma_2}{\overset{\hat{\Gamma}_m(t)=\Gamma_1}{\gtrless}} 0 \\
&\Leftrightarrow \cos\left(\phi - \underline{\angle y_m\left[\Gamma_1\right] - y_m\left[\Gamma_2\right]}\right) \underset{\hat{\Gamma}_m(t)=\Gamma_2}{\overset{\hat{\Gamma}_m(t)=\Gamma_1}{\gtrless}} 0
\end{aligned} \tag{2.16}$$

Given the relation in Eq. (2.15), the optimal load sequence $\hat{\mathbf{\Gamma}}^{\mathrm{opt}}$ can be found by varying ϕ from 0 to 2π. It is further noticed that, as ϕ scans $[0, 2\pi)$, the decision $\hat{\Gamma}_m(t)$ changes, according to Eq. (2.16), only when:

$$\cos\left(\phi - \underline{\angle y_m\left[\Gamma_1\right] - y_m\left[\Gamma_2\right]}\right) = 0 \Leftrightarrow \phi = \underbrace{\pm\frac{\pi}{2} + \underline{\angle y_m\left[\Gamma_1\right] - y_m\left[\Gamma_2\right]} \pmod{2\pi}}_{\phi_m^{(1)},\phi_m^{(2)}}. \tag{2.17}$$

Therefore, the sequence $\hat{\mathbf{\Gamma}} = \left[\hat{\Gamma}_1(t), \hat{\Gamma}_2(t), \ldots, \hat{\Gamma}_M(t)\right]^T$ changes only at

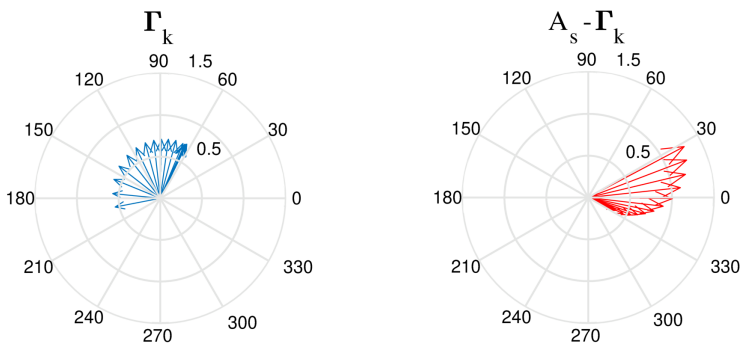
$$\left(\phi_1^{(1)}, \phi_1^{(2)}, \phi_2^{(1)}, \phi_2^{(2)}, \cdots, \phi_M^{(1)}, \phi_M^{(2)}\right).$$

For the remaining part of this section, we assume that the above $2M$ points are distinct and nonzero, i.e., $\phi_m^{(j)} \neq \phi_l^{(k)}$ and $\phi_m^{(j)} \neq 0$, for any $j, k, \in \{1, 2\}$ and $m, l \in \{1, 2, \ldots, M\}$ with $m \neq l$. There is a case where the above assumption does not hold, examined in [57]. If the above points are sorted in ascending order, i.e.,

$$(\theta_1, \theta_2, \cdots, \theta_{2M}) = \mathsf{sort}\left(\phi_1^{(1)}, \phi_1^{(2)}, \phi_2^{(1)}, \phi_2^{(2)}, \cdots, \phi_M^{(1)}, \phi_M^{(2)}\right), \tag{2.18}$$

then the decision $\hat{\mathbf{\Gamma}}$ will remain constant in each one of the $2M + 1$ intervals $(\theta_i, \theta_{i+1}), i \in \{0, 1, \ldots, 2M\}$, with $\theta_0 = 0$ and $\theta_{2M+1} = 2\pi$. The goal is the identification of the $2M + 1$ sequences that correspond to these intervals,[3] one of which

[3]It can be shown that the sequence at $[0, \theta_1)$ is the same with the sequence at $[\theta_{2M}, 2\pi)$ and thus,



(a) (b)

Figure 2.1: The 21 reflection coefficients used in the simulations.

gives the optimal $\hat{\mathbf{\Gamma}}^{\text{opt}}$, i.e., the one that offers the maximum power; thus, the quality of each sequence is calculated with the norm metric of Eq. (2.14), which explicitly includes the direct channel h_0. Based on the above, the sorting operation in Eq. (2.18) is dominant in terms of computational cost, which is $\mathcal{O}(M \log M)$ and not 2^M.

2.4 $K > 2$ Loads

The method described above can be generalized to $K > 2$ loads, i.e., $\Gamma_m(t)$ belongs in $\{\Gamma_1, \Gamma_2, \ldots, \Gamma_K\}$. The solution is given by selecting the largest value of $\Re\left\{e^{-j\phi} y_m[\Gamma_k]\right\}$ among all $k \in \{1, 2, \ldots K\}$, which results in testing $2M \times (K-1)$ changes of ϕ and as a result, same number of sequence changes and not $2M \times \binom{K}{2}$, as one would expect; the rest of the steps are exactly the same as in $K = 2$. Formal proof and details can be found in [57]. Notice that the norm metric for the quality of each sequence must include h_0. The complexity of the algorithm is not K^M, but again $\mathcal{O}(M \log M)$ for $M > K$.[4].

Fig. 2.1a depicts $K = 21$ (complex) reflection coefficients, corresponding to the 21 loads, offered through a varactor at each tag, as experimentally tested in [59]. It can be shown that these reflection coefficients span more than 120°. Fig. 2.1b shows $A_s - \Gamma_k, k \in \{1, 2, \ldots K\}$, which incorporates the contribution of the structural mode of each RIS element antenna, typically overlooked in the literature; it can be seen that the span of $A_s - \Gamma_k$ in degrees is much smaller, in the order of 60°.

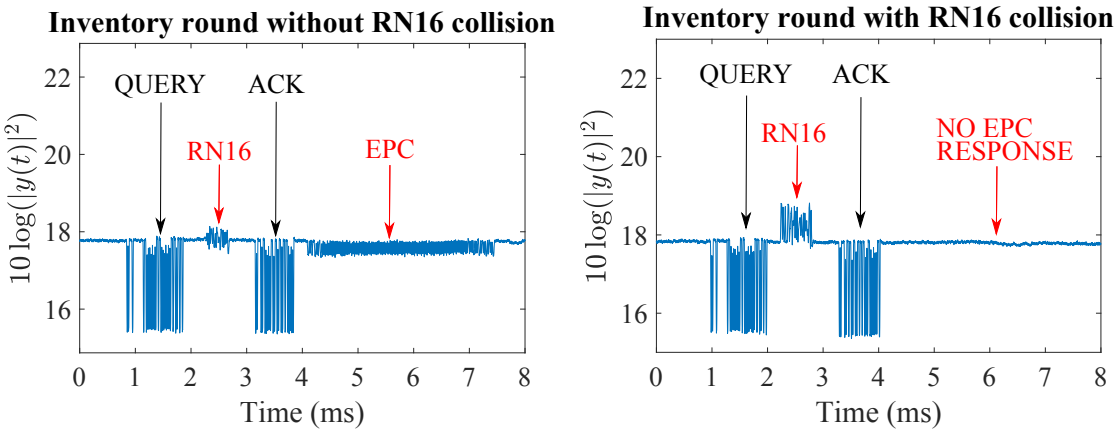
$2M$ intervals/sequences should be identified.

[4]During writing, work in [58] was found, which however offers suboptimal gain for $K > 2$ loads per element; for $K = 2$ loads, the algorithm there requires sorting of $2M + 2$ phases [58, page 970, first column, definition of $2M + 2$ arcs in $[0, 2\pi)$], and thus obtains complexity of $\mathcal{O}(M \log(M))$.

Chapter 3

Wireless Batteryless Implementation with RFIDs

The RFID-based RIS is controlled by the RFID reader at carrier frequency f_2, through commands such as Select, Query and ACK, explained below. In the commercial RFID standard (EPC Gen2), a framed slotted Aloha (FSA) protocol is used, so that tags backscatter one at a time, without collision. For RIS purposes, the opposite is needed, i.e., tags must be forced to backscatter in carefully selected groups.



(a) No RN16 collision.

(b) RN16 collision.

Figure 3.1: Conventional Gen2 RFID operation from experimental measurements: each tag responds to a Query command with a random RN16 message; if it is correctly acknowledged, it will respond with its EPC.

In Gen2, the reader initiates the start of a frame with a Query command, which contains the number of slots. Ideally, the number of slots should be equal to the number of tags to be inventoried. If the reader advertises number of slots equal to 1, then all tags in the vicinity of the reader will respond. That was the approach followed in this work. Then, each tag responds with a random 16-bit number, namely the RN16 message, which is in principle different among the competing tags. If the reader correctly decodes that message then it will send the ACK command, containing the RN16 sent by the tag. Collision detection and error detection is conducted at

the reader using the line coding the tags incorporate (FM0 or Miller).[1] If the tag is correctly acknowledged, it will reply with its ID (EPC); the latter is typically 96−bits payload plus CRC bits. Fig. 3.1a depicts an inventory round with an acknowledged tag, while in Fig. 3.1b multiple tags have backscattered their RN16, resulting to a collision; this is the case exploited in this work.

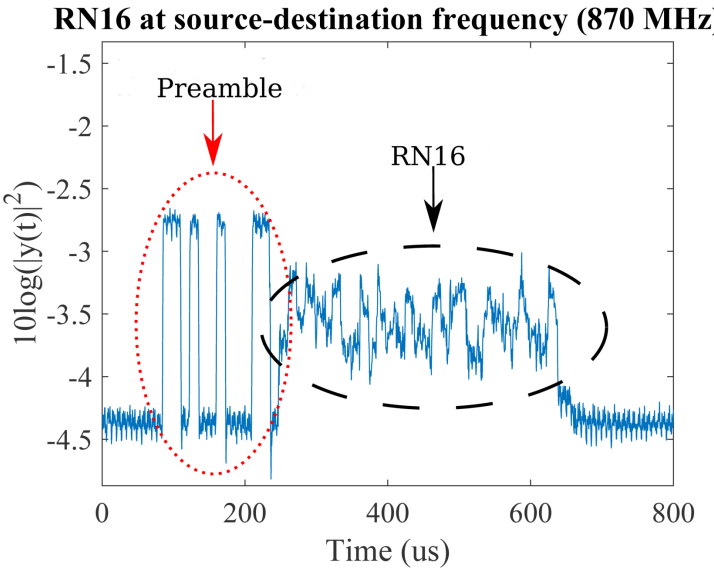


Figure 3.2: Superposition of Preamble+RN16 from multiple tags.

The RN16 is preceded by a 6-bit Preamble sequence, which does not follow the line coding rules and is the same for all tags. As a result, using the Preamble one could measure the effect of a specific RIS *configuration* (where configuration denotes the set of tags that change their reflection coefficients, among the total number of RIS tags). Since the random 16-bit sequence of the RN16 is different for each tag, the signal level (or the effective channel) during RN16 could be higher or lower than the Preamble level because only a subset of the configuration's tags are terminated at the same load at a given point of time. This is shown in Fig. 3.2.

In the Gen2 industrial RFID standard, the Select command (issued by the Reader) is asserting or deasserting the SL flag of the tags. When a tag has its SL flag asserted, it responds with an RN16 after a Query command. The Select command contains a mask with a specified length and starting point. Each tag compares this mask with its corresponding EPC bits. The Action parameter, which is a field set by the reader during the Select command, allows the user to specify how the SL flag will change if the mask matches the EPC of the tag. To assert a specific tag's SL flag without

[1]The reader directs the tags about the line code they are going to use.

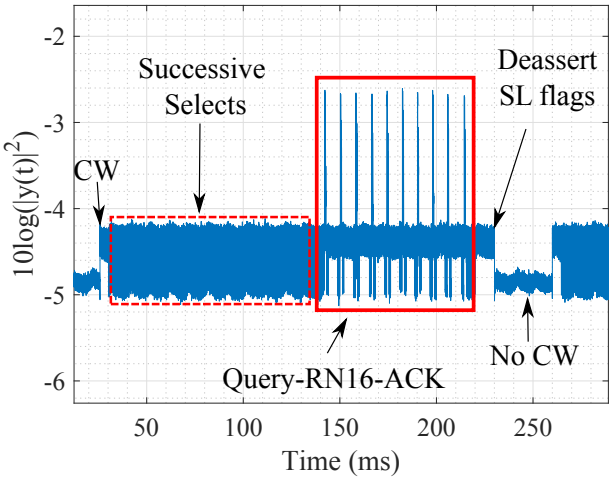


Figure 3.3: Reader-Tag communication during a configuration.

affecting the others', the Action parameter is set to $\{0, 0, 1\}$. To deassert all SL flags with one Select, the Action parameter is set to $\{0, 0, 0\}$ and the mask is set to avoid corresponding to any tag.

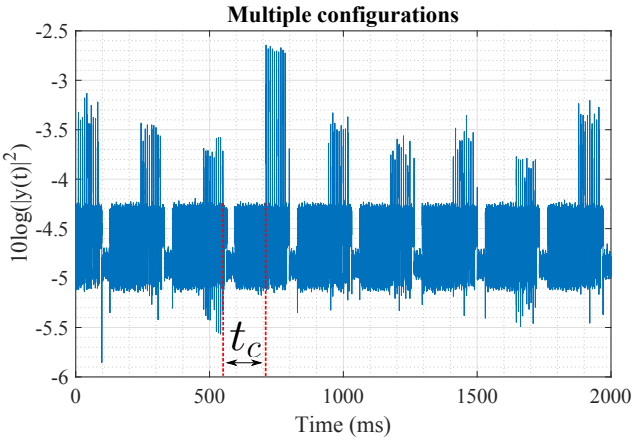


Figure 3.4: Power at Destination during different configurations.

For RIS purposes, a *specific* configuration is set by having the reader issuing successive Select commands and asserting the SL flag of the specified tags, sequentially. This is shown in Fig. 3.3. First, a continuous wave (CW) energizes the tags and then the Select commands are issued. Afterwards, we can observe 10 inventory rounds (Query-RN16-ACK), where the peaks are the superposition of the RN16 from the selected tags. Finally, to advance to a new configuration, another Select is sent but with Action parameter equal to $\{0, 0, 0\}$ and a non-matching mask to any tag.

In Fig. 3.4 we observe a sequence of 9 different configurations. Each configuration

spans 10 inventory (Query-RN16-ACK) rounds. Different configurations offer different effective channel and hence, different maximum signal power. Those peaks occur at the Preamble+RN16 tag response, as explained in Fig. 3.3. It is noted that the measurements were conducted in a static indoor environment, with channel coherence time spanning several hundreds of msec (and thus, different peaks are due to different tag configurations and not changes in the channel). The time between the end of the last RN16 from one configuration and the start of the first RN16 from the next is specified as t_c. More specifically, by varying the backscatter link frequency (BLF) parameter, t_c changes accordingly. The dependence of t_c in number of tags selected at each configuration, is better explained by the following equation:

$$\begin{aligned} t_c &= (\mu+1)\left(\mathrm{T_{SELECT}}+\mathrm{T_4}\right)+\mathrm{T_{DELAY}}+\mathrm{T_{PU}} \\ &= (\mu+1)\left(61\cdot\frac{1}{\mathrm{BLF}}\cdot 10^3+0.15\mathrm{ms}\right)+30\mathrm{ms}\ +184\cdot\frac{1}{\mathrm{BLF}}\cdot 10^3 \end{aligned} \tag{3.1}$$

In Eq. (3.1), μ is the number of activated elements/tags in a configuration with μ Select commands asserting the SL flags and, at the end of the configuration, one deasserting them; $\mathrm{T_{SELECT}}$ is the duration of a Select and $\mathrm{T_4}$ is the minimum duration between successive reader commands; $\mathrm{T_{DELAY}}$ is a time interval at the end of the configuration where no commands or continuous wave (CW) is transmitted by the reader, shown in Fig. 3.3. This allows the tags to deassert their SL flags and was found heuristically for the specific RFID tags used, in the order of 30ms; backscatter-Link frequency BLF $\in$ [40 kHz, 640 kHz] was set in the experimental setup equal to 40kHz. For time T_{PU}, the reader sends CW prior to the Select command to power-up the tags and set them to the Ready state. By varying the BLF parameter, t_c changes accordingly. For example, if $\mu = 50$, then $t_c \in [43\ \mathrm{ms}, 116\ \mathrm{ms}]$. In Fig. 3.4, $t_c = 116$ ms. Future RIS-friendly modifications of Gen2 could further reduce this parameter. For example, parameter $\mathrm{T_{DELAY}}$ should be decreased, the Select command should be reduced in size and parameter BLF should be increased as much as possible.

The experimental setup is depicted in Fig. 3.5, with M = 100 commodity Alien ALN-9840 Gen2 RFID tags , separated by $d_x = 10$ cm and $d_y = 5$ cm. The source-destination link operates at $f_1 = 870$ MHz, while the software-defined radio reader operates at $f_2 = 866$ MHz, with zero interference among the two channels. Modifications in the Gen2 reader software stack from [60] were conducted to enable RIS functionality. Two commodity USRP N200 software defined radios, each equipped with a RFX900 daughterboard, were utilized, both connected to a commodity laptop

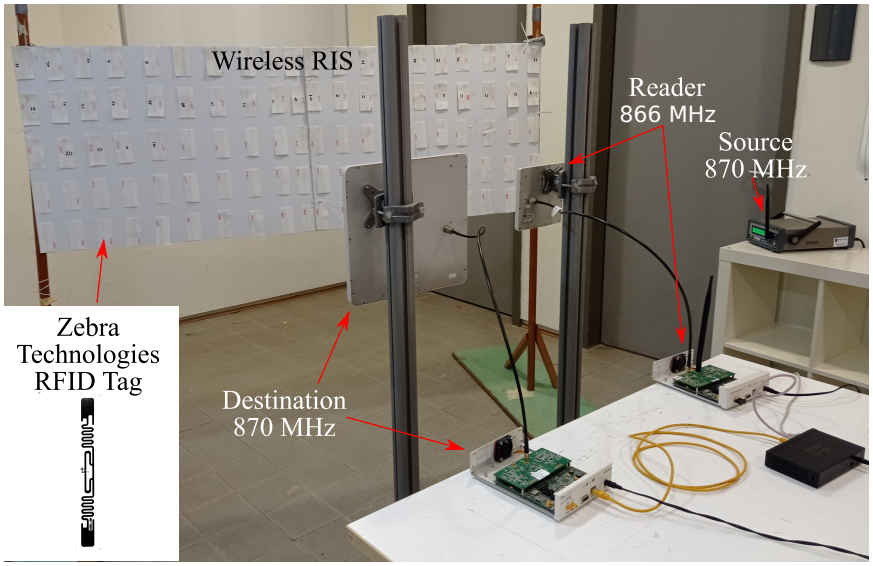


Figure 3.5: Experimental setup.

through a switch. One SDR was used as the Reader that controlled the RIS tags and the other was utilized as the destination. Source of the link was a signal generator at 870 MHz. The antennas used at the reader and source were circularly-polarized. It is emphasized that Figs. 3.1, 3.2, 3.3, 3.4 are offered from the SDR receiver at the destination.

Gen2 RFIDs are exploited as batteryless, wirelessly controlled reflective elements. Each RFID label requires an impinged RF power greater than its sensitivity threshold. In the case of the utilized ALN-9840 tags, an RFID reader should (typically) provide at least -17.8 dBm (-14.8 dBm if write operations are required) of RF power at the location of each tag [61].

Chapter 4

Numerical Results

4.1 Simulations

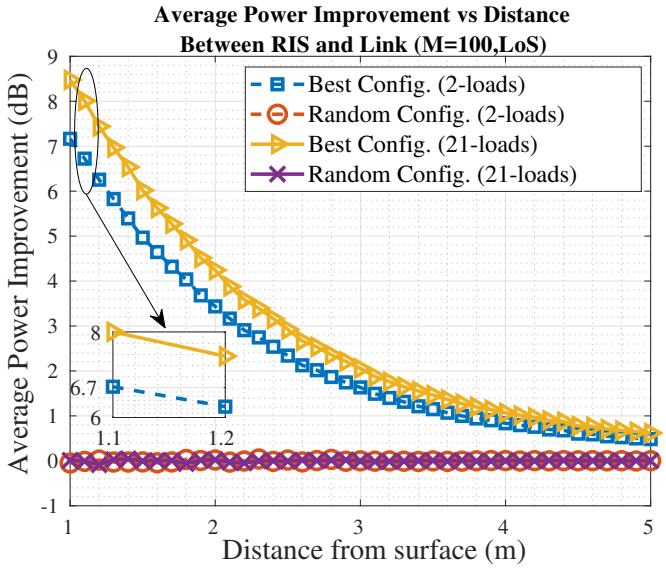


Figure 4.1: Average Power Gain; tags' spacing $d_x = d_y = \frac{\lambda}{2}$.

Figs. 4.1 and 4.2 are generated with typical indoor static conditions in mind: $\kappa_{\mathrm{ST}_m} = \kappa_{\mathrm{T}_m\mathrm{D}} = \kappa_{\mathrm{SD}} = \kappa = 8$, $v_{\mathrm{X}} = 3$; moreover, $\eta = 10\%$, $d_0^{\mathrm{X}} = d_{\mathrm{SD}} = 3$ m, $f_2 = 870$ MHz, $P = 5$ dBm, and 10 dB relative end-2-end antenna gain for the backscattered links compared to direct link, assuming that the source and destination antennas point towards the RIS, assisting its operation.

Fig. 4.1 offers the average power improvement due to RIS and direct link operation, compared to direct link communication only (without RIS). Several instances of the channels are generated, optimal configuration is found, for $K = 2$ or $K = 21$ loads per element and $M = 100$ RIS elements, based on the analysis of Section 2.2 and the average power improvement is reported. The SD link is parallel to RIS and distance from surface ($d_{\mathrm{RIS-SD}}$) is varied. It is noted that exhaustive search among $K^M = 2^{100}$ or 21^{100} configurations among RIS elements is practically impossible; however, results are offered based on the optimal gain discovery algorithm of Section 2.2. It is observed

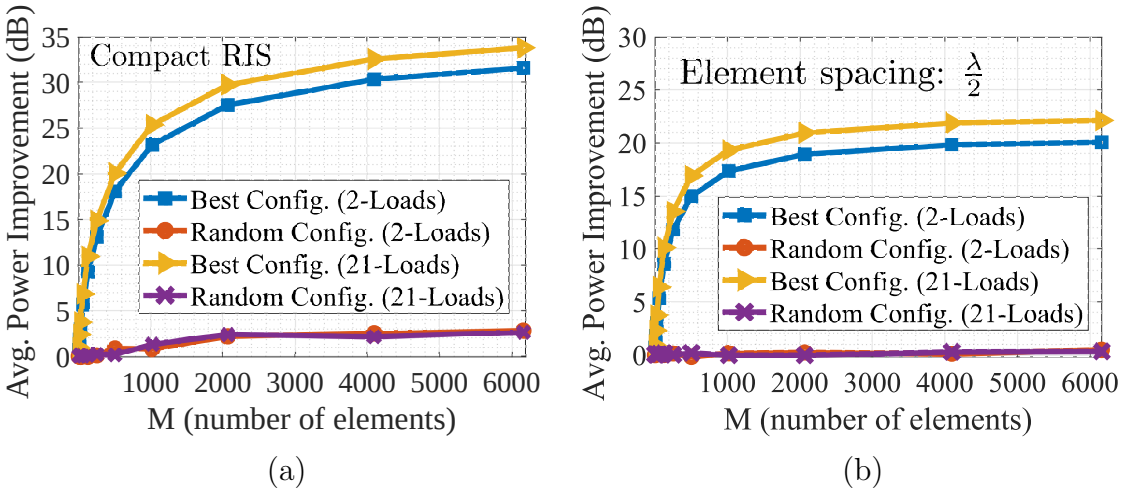


Figure 4.2: Average power improvement (dB) vs number of RIS elements M.

that as the distance of the SD link from RIS increases, performance gains of optimal RIS operation decrease. That is due to the fact that backscattered links (through RIS) become weaker, as the distance of the SD link from the surface increases. This finding suggests that amplification at each RIS element (i.e., $|\Gamma_k| > 1$), i.e., *active* rather than passive RIS operation is needed; it is also important to carefully model the wireless channel, as well as the backscattering operation. Moreover, it is observed that using $K = 21$ loads for each element, despite the small angle span of the induced backscattered signals (explained in Sec. 2.4), offers power gain in the order of 1.3 additional dB only, compared to $K = 2$. Perfect CSI is assumed in this figure, as well as in next Fig. 4.2 and Fig. 4.3.

Fig. 4.2 offers average power improvement as a function of M, for two setups: Fig. 4.2a sets $d_x = 0.1$ m $< \lambda/2$ and $d_y = 0.05$ m $< \lambda/2$ (setup (a)), while Fig. 4.2b sets spacing between adjacent tags equal to $\lambda/2 = 0.172$ m (setup (b)). For both setups, $d_{\text{SD}} = 3$ m, $d_{\text{RIS-SD}} = 1$ m, while setup (a) ignores possible coupling between adjacent tags. It is found that performance in setup (b) reaches a plateau with a faster rate than in (a), as a consequence of the larger element spacing. This finding suggests that even with perfect channel estimation, the weak nature of backscattered links limits the performance gains, even for large number of tags/RIS elements, in the order of $M = 6000$.

Fig. 4.3 shows a comparison of the average power improvement of the proposed algorithm versus a majority voting algorithm for $K = 2$ loads per RIS element, proposed in [1]. The distances are $d_{\text{RIS-SD}} = 1$ m, $d_{\text{SD}} = 3$ m and the element spacing is $d_x = \lambda/2$ and $d_y = \lambda/2$. Also, the transmission power is $P = 20$ dBm, $\eta = 10\%$ and

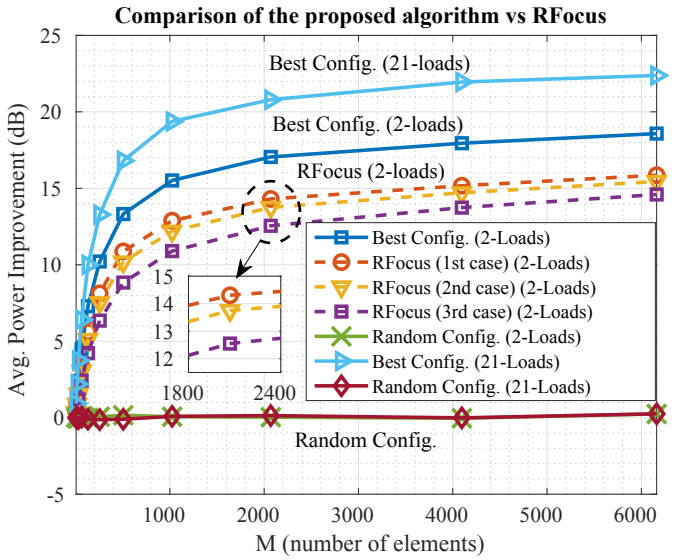


Figure 4.3: Comparison of the proposed algorithm ("Best Config.") vs a majority voting algorithm [1].

$\kappa = 8$. The algorithm in [1] is feedback-based and uses K_r feedback measurements to decide which elements contribute constructively. Fig. 4.3 offers three cases: 1st case with $K_r = \left\lceil \frac{3(M+1)}{2} \right\rceil$, 2nd case with $K_r = M+1$ and 3rd case with $K_r = \lceil \frac{M+1}{2} \rceil$, where M is the number of RIS elements. Parameter K_r was chosen proportionally to the total number of channels $M+1$, with the underlying assumption that estimation of all channel coefficients in this work incurs a time overhead similar to the K_r feedback measurements. Fig. 4.3 shows that the proposed algorithm has a greater average power improvement for $K = 2$ loads. Also, it can further enhance its performance by using tags with $K > 2$ loads. In addition, the algorithm in [1] has a complexity of $\mathcal{O}(MK_r)$ and it is required that $K_r \geq M$, so that a well-determined problem is crafted. The proposed algorithm is computationally more efficient, given that it has a complexity of $\mathcal{O}(M \log M)$ compared to $\mathcal{O}(MK_r)$, while it can efficiently find the optimal configuration even for $K > 2$ loads per RIS element. A specific example with $K = 21$ loads for the proposed algorithm is also depicted.

It is noted that both Figs. 4.2, 4.3 demonstrate that a quadratic scaling law of M^2 for the beamforming gain is not in place. This is not surprising, since as the number M of RIS elements increases, the distance of certain RIS elements from source or destination (of the SD link) also increases and hence, their contribution to the aggregate signal diminishes. The quadratic scaling law is valid only when the signal amplitude from each contributing element remains constant, as M increases, which is clearly not the case in realistic setups.

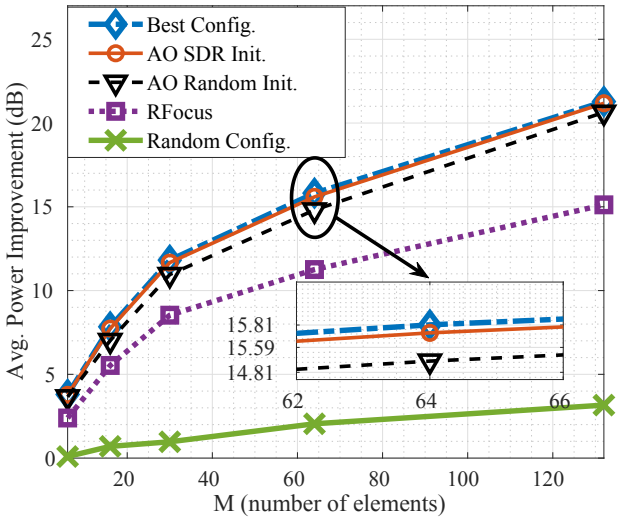


Figure 4.4: Proposed algorithm ("Best Config.") vs suboptimal methods.

Fig. 4.4 presents a comparison between the proposed algorithm and state-of-the-art methods [1], [62], [63]. Alternative optimization (AO) with semi-definite relaxation-based initialization or random initialization are tested [62], [63]; with such AO, each element's estimated load is determined in an iterative manner, solving for each element separately, while fixing all the other elements' loads. Proper initialization of the elements' phase shifts is required. AO Random Init. depicts the performance of the AO algorithm with random initialization and the AO SDR Init. with quantization of the continuous phases obtained from [62], to the nearest discrete loads' phases. Perfect CSI is assumed with $\kappa = 3$, $v_{\mathrm{X}} = 3$; moreover, $\eta = 10\%$, $d_0^{\mathrm{X}} = d_{\mathrm{SD}} = 3$ m, $f_2 = 870$ MHz, $P = 5$ dBm, and 20 dB relative end-2-end antenna gain for the backscattered links compared to direct link. Also, for the RFocus algorithm $K_r = M + 1$. All the algorithms depicted are for $K = 2$ loads of constant amplitude and difference in phase equal to π.

Based on Fig. 4.4 it is observed that the proposed algorithm outperforms both AO schemes and RFocus and provides the optimal solution. Furthermore, the SDR problem that initiates the loads of the AO SDR Init. has significant computational complexity in the number M of RIS elements of at least $\mathcal{O}(M^{3.5})$ due to the utilized semi-definite relaxation, which is prohibitive for large intelligent surfaces (i.e., large M). That is why the figure is limited to a relatively small M, up to $M = 132$. In sharp contrast, the proposed algorithm conveniently scales up to a large number of elements M, in the order of hundreds to thousands, due to its attractive $\mathcal{O}(M \log(M))$ computational complexity. Additionally, the formulation of [62] and [63] assumes a common

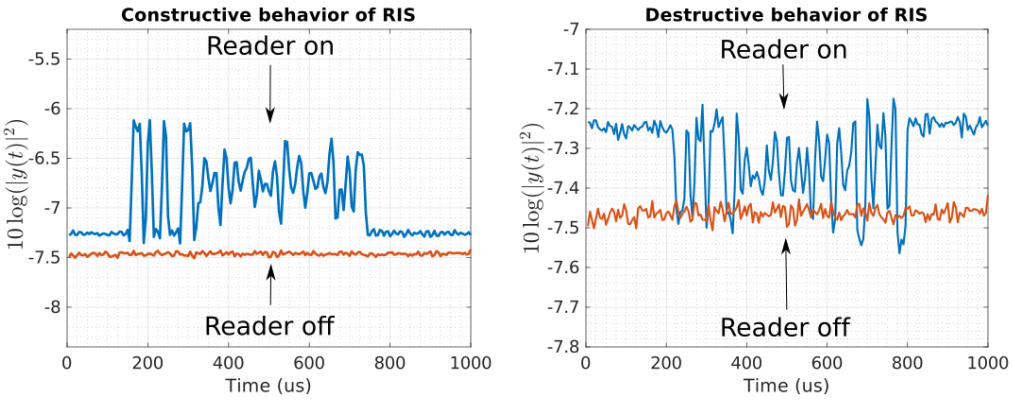


Figure 4.5: Received signal strength at the destination: constructive vs destructive RIS impact.

constant amplitude reflection coefficient across all elements, which may not be the case in practical RIS designs and implementations. The proposed scheme is more general, since it can accommodate *any* set of reflection coefficients, not necessarily of common amplitude.

4.2 Experiments with the Wireless, Batteryless Testbed

For the purposes of channel estimation, the reflective elements are required to terminate their antenna at loads attaining the values of A_s and 0. Unfortunately, the commercial RFIDs we utilized as RIS elements do not support $\Gamma = A_s$. In addition, the exact loads of the RFID tag are not readily available. Thus, a different validation approach was adopted.

Fig. 4.5 offers the received power at the destination, operating @ 870 MHz, with the setup of Fig. 7 for two different configurations. With the reader on (@ 866 MHz), both the RIS and the SD link contribute to the received power (@ 870 MHz). With the reader switched off, the received power at the destination is measured and depicted. Clearly, one configuration offers constructive and another destructive RIS operation. The source-RIS distance was denoted as $d_{\text{RIS}-\text{S}}$ and the destination-RIS as $d_{\text{RIS}-\text{D}}$, measured from the RIS center; these parameters are the same as in Fig. 4.6.

Fig. 4.6 shows the maximum power improvement achieved as a function of number of configurations tested, for variable number of activated tags (denoted by μ). The setup corresponds to $d_{\text{RIS}-\text{S}} = 2.4$ m, $d_{\text{RIS}-\text{D}} = 1$ m and $d_{\text{SD}} = 2.1$ m. For a given

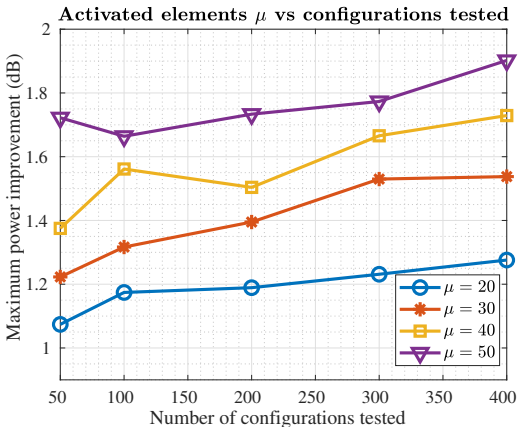


Figure 4.6: Maximum power improvement vs Number of configurations tested for several μ.

configuration and μ, the value reported is over five repetitions. Increasing the number of configurations tested results to an increased maximum power value, on par with the simulation results. It is noted that the relatively small number of RIS elements/RFID tags tested, can only offer a small power improvement. Also, when μ is increased, the maximum gain is increased for a given number of configurations.

Fig. 4.8 offers the maximum power gain improvement, measured for three different source positions, over 1000 random configurations. For these experiments, a new RIS was established, consisting of $M = 256$ tags with $d_x = 5.25$ cm and $d_y = 5$ cm. The experiment was repeated for $\mu = \{64, 128, 192\}$ and for $P = \{0, 10\}$ dBm. The rest of the setup is kept static. Also, to reduce the amount of interference at the destination link, the reader was moved to 920 MHz. The individual distances for the three different source positions tested are listed in Table 4.1 and a schematic of the setup is depicted in Fig. 4.7. Results of these experiments are offered in Fig. 4.8.

d_X (m) / Position	d_{SD}	$d_{\text{RIS-S}}$	$d_{\text{RIS-D}}$
1	2.10	3.22	1.09
2	2.24	3.18	1.09
3	3.25	4.02	1.09

Table 4.1: Distances for the positions of Fig. 4.8.

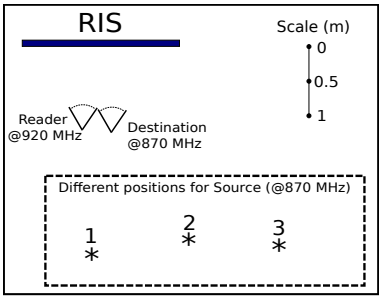


Figure 4.7: Top view of the setup of Fig. 4.8.

Fig. 4.8 shows that the maximum gain improvement is highly associated with

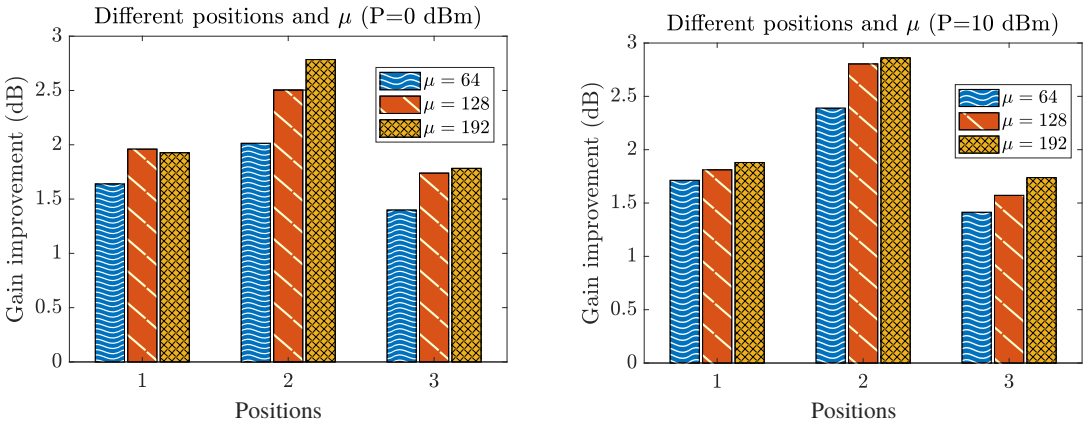


Figure 4.8: Maximum power improvement for various positions and μ values ($P = \{0, 10\}$ dBm).

the position of the source link, since position 2 has the maximum gain for each value of μ. This leads to the conclusion that the channels have a dominant effect on the RIS operation and can either enhance or limit its performance. Also, increasing the number of effective tags μ is systematically improving the RIS performance, which shows that future applications should incorporate a higher number of tags (order of thousands) to achieve maximum gains. Additionally, varying the transmission power of the source P did not show any dramatic effect on the operation of the RIS.

Chapter 5

Passive radar overview

In this chapter, some basic passive radar theory is presented along with an overview of the individual components that comprise the developed PBR system. This chapter is based on [19], [46], [64].

5.1 Background

The geometry of the PBR is described in Fig. 5.1, where the transmitter j and the receiver i, are the foci of an ellipse where the target's position lies. The target's 3D velocity vector $\mathbf{v}$ is, also, depicted.

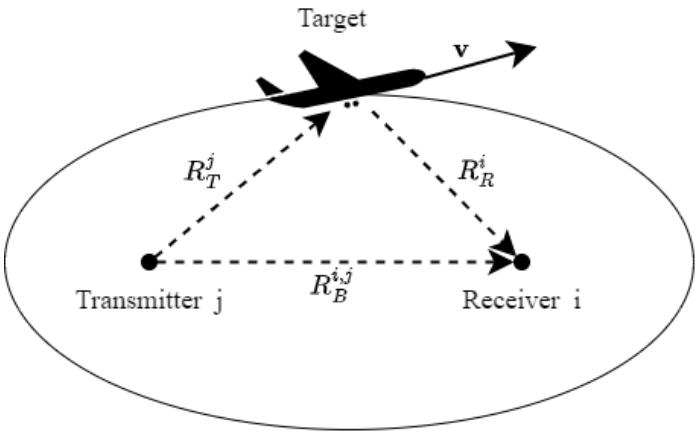


Figure 5.1: Bistatic radar geometry.

5.1.1 Bistatic Range

The bistatic range between the jth transmitter located at (x_T^j, y_T^j, z_T^j), a target at (x, y, z) and the ith receiver at (x_R^i, y_R^i, z_R^i) is computed by first measuring the distance from the transmitter to the target:

$$R_T^j = \sqrt{(x - x_T^j)^2 + (y - y_T^j)^2 + (z - z_T^j)^2}, \tag{5.1}$$

from the target to the receiver:

$$R_R^i = \sqrt{(x - x_R^i)^2 + (y - y_R^i)^2 + (z - z_R^i)^2} \tag{5.2}$$

and the baseline distance which is:

$$R_B^{i,j} = \sqrt{(x_T^j - x_R^i)^2 + (y_T^j - y_R^i)^2 + (z_T^j - z_R^i)^2}. \tag{5.3}$$

Then, the bistatic range becomes:

$$R_{ij} = R_T^j + R_R^i - R_B^{i,j}. \tag{5.4}$$

The bistatic range R_{ij} is obtained by the time delay τ, which is the delay between the target's echo and the reference signal calculated as follows:

$$R_{ij} = c\,\tau, \tag{5.5}$$

with c the speed of light. An ellipsoid is formed from that delay, with the transmitter j and receiver i at its foci.

5.1.2 Bistatic Velocity

The bistatic velocity between the jth transmitter, a target moving with speed vector $\mathbf{v} = [\dot{x}, \dot{y}, \dot{z}]^T$ in the three-dimensional (3D) space and the ith receiver is given as follows:

$$V_{ij} = \frac{(x - x_T^j)\dot{x} + (y - y_T^j)\dot{y} + (z - z_T^j)\dot{z}}{R_T^j} + \frac{(x - x_R^i)\dot{x} + (y - y_R^i)\dot{y} + (z - z_R^i)\dot{z}}{R_R^i}. \tag{5.6}$$

The bistatic velocity is calculated by measuring the Doppler frequency shift $f_d^{i,j}$ of the target's echo relative to the reference signal, transmitted from the jth transmitter and received from the ith receiver. The formula is listed below:

$$V_{ij} = -\lambda_j\, f_d^{i,j}, \tag{5.7}$$

where the wavelength of the jth transmitter is $\lambda_j = \frac{c}{f_c^j}$, with f_c^j the jth transmitter's carrier frequency.

5.2 System Model

A PBR system captures the transmitted signal in various forms, shown in Fig. 5.2.

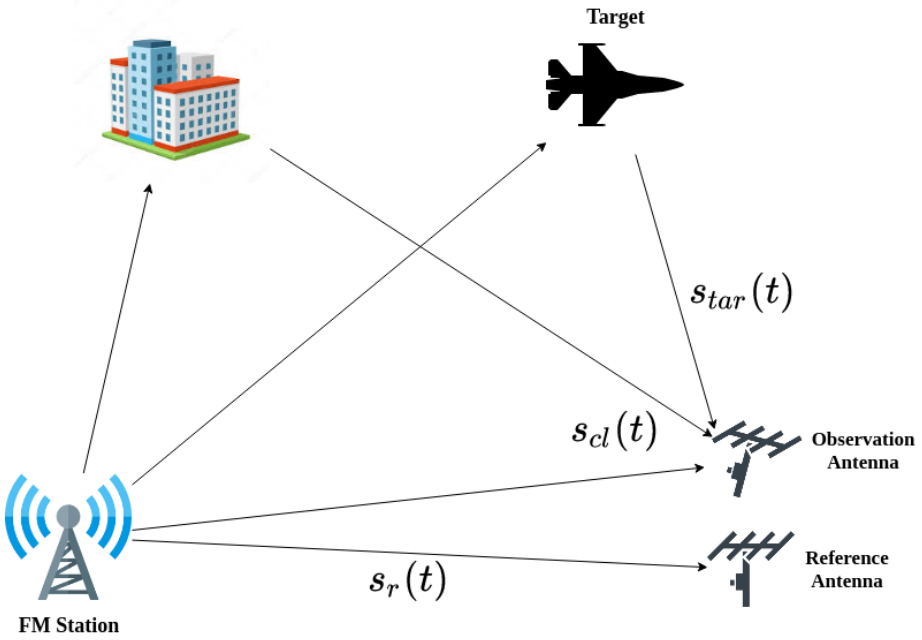


Figure 5.2: The various paths of the transmitted signal prior to PBR capturing.

The observation antenna receives a signal $s_o(t)$, which could be analysed to its individual components as follows:

$$s_o(t) = s_{cl}(t) + s_{tar}(t) + v_o(t), \tag{5.8}$$

where $s_{cl}(t)$ is the clutter, $s_{tar}(t)$ is the target's reflection and $v_o(t)$ is additive complex white Gaussian noise. Clutter is comprised from the direct signal leakage (DSI) and multipath reflections of the transmitted waveform in various surfaces, such as buildings, mountains etc. as shown in Fig. 5.2. The target's reflection is a relatively weak signal, that arrives with a certain delay and Doppler shift.

The reference antenna receives the following signal:

$$s_r(t) = A_r\, s_{tx}(t - \frac{R_B}{c}) + v_r(t), \tag{5.9}$$

with $s_{tx}(t)$ the FM station's transmitted signal, a scaling parameter A_r corresponding to the channel's impact and R_B the baseline distance between the FM station and the PBR. For the rest of the analysis, it is assumed that the received signal $s_r(t)$ is equal to $s_{tx}(t)$, along with its discrete-time counterparts, $s_r[n]$ and $s_{tx}[n]$. This is considered

a relatively accurate assumption when there is line-of-sight (LOS) reception of the transmitter's signal by the reference antenna.

A more analytical form of the observation signal model of Eq. 5.8 is given in discrete-time, where samples are generated with a sampling frequency of $F_s = 1/T_s$, as follows:

$$s_o[n] = \underbrace{\sum_{k=0}^{M-1} w_k \, s_r[n - d_{cl,k}]}_{\text{clutter}} + \underbrace{\sum_{l=0}^{N-1} b_l \, s_r[n - d_{e,l}] \exp\left(\frac{j\,2\pi\, f_{e,l}\, n}{F_s}\right)}_{\text{target reflections}} + v_o[n], \tag{5.10}$$

with clutter comprising of M discrete paths with the kth path having a complex amplitude w_k and a delay $d_{cl,k}$ that corresponds to the channel's effect. Also, there are N targets present in the observation area. The lth target reflection has complex amplitude b_l, delay $d_{e,l}$ and an exponential term due to the Doppler frequency $f_{e,l}$. In addition, there is additive complex Gaussian noise, modelled by the term $v_o[n]$.

Then, $s_r[n]$ is used to extract any unwanted clutter from the observation signal, as follows:

$$s_{tar}[n] = s_o[n] - \sum_{k=0}^{M-1} w_k \, s_r[n - d_{cl,k}] + v_o[n]. \tag{5.11}$$

Both the clutter and the target reflections are scaled and delayed replicas of the reference signal $s_r[n]$; $s_{cl}[n]$ can be separated from $s_{tar}[n]$ due to the target's Doppler shift and, more specifically, due to the orthogonality principle between appropriately frequency shifted signals, as described in [64]. Removing $s_{cl}[n]$ requires appropriate values for each w_k term, which corresponds to a delay $d_{cl,k}$. This is the topic of Sec. 5.4.1. Successful removal would reduce the range-Doppler sidelobe levels, thus enabling target detection.

5.3 Experimental Setup

The system comprises of two high gain antennas, a Yagi-Uda (Fig. 5.3) with 3 elements, as the reference and a custom made 5 element small Yagi-Uda [65] antenna (Fig. 5.4), as the observation antenna.

The reference antenna has LOS with the transmitters for optimal performance and is mounted on the roof of the School of Electrical and Computer Engineering building in TUC. On the other hand, DSI and clutter are major limiting factors in

Figure 5.3: Reference antenna.

Figure 5.4: Observation antenna.

the PBR's performance. A method to mitigate this problem is by properly placing the antenna in such a way to shield it from unwanted signal leakage. This involves angular nulling, where the antenna is carefully steered in order to find the lowest DSI level while, also, by using large surfaces such as buildings as RF shielding. This methods help to reduce the amount of clutter received by the observation antenna.

The I/Q baseband samples for both $s_r[n]$ and $s_o[n]$ are captured with the help of a Lime software-defined radio (SDR)-LimeSDR (connected through USB to a laptop), depicted in Fig. 5.5, also exploiting the GNURadio software framework. This type of SDR has 2 receivers, capable of simultaneous and synchronous reception. Its ADC resolution is 12 bits, thus enabling moderate clutter removal and PBR performance.

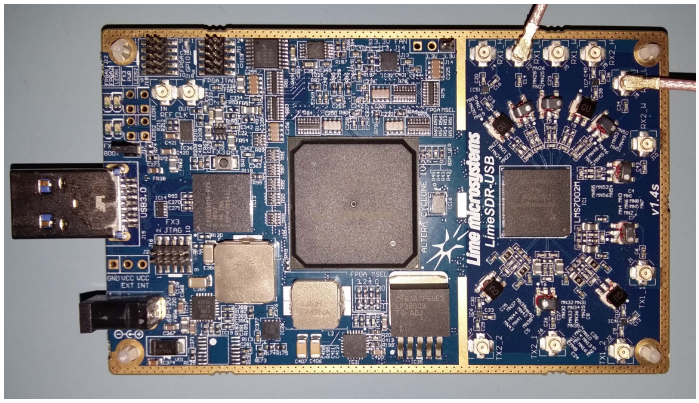


Figure 5.5: The LimeSDR USB used.

5.4 Signal processing

The processing on each passive radar (PR) node is depicted in Fig. 5.6.

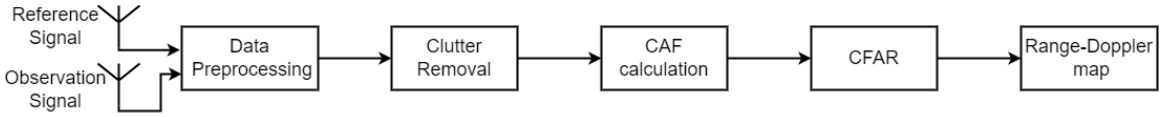


Figure 5.6: Stages of the PR processing.

Two RF chains drive both the reference, looking directly towards the illuminator of opportunity (IoO), and the observation signal, which is directed towards the target and contains its echo plus clutter.

Then, some initial preprocessing takes place, which includes filtering each channel of interest by moving the input central frequency to the channels central frequency, decimating the IQ samples to match the channels' bandwidth, removing any sample offsets between the two RF chains etc.

5.4.1 Clutter removal

Next, clutter removing from the observation signal is a crucial step in passive radar processing. The cross-correlation between the reference and the observation signal creates a very strong peak around $|\chi(0,0)|$, i.e., where most of the direct signal leakage (DSI) occurs. This phenomenon introduces unwanted sidelobes to the Range-Doppler surface, which mask the target's weak signal. Reflections on the earth's surface, sea, buildings, moving cars or trees etc. only exacerbate the problem, thus making clutter removal a necessity.

The basic assumption in order to remove the DSI is that, as shown in Eq. 5.10, it is a scaled and delayed replica of the reference signal. In other words, any DSI or clutter due to reflections in general, is mainly due to static or nearly static objects. This is in contrast to the velocities of civil aircraft for example, where Doppler shifts can reach tens or hundreds of Hz to the central frequency. Therefore, removing clutter would require to find the correct amplitudes w_k of Eq. 5.10 on each delayed replica of the reference signal.

The algorithms used in this thesis were based on [64], where a comparison of the performance and computational cost of the least squares (LS), normalized least mean squares (NLMS) and fast block NLMS (FBNLMS) was performed. The results showed that NLMS was the better performing algorithm in terms of clutter removing and FBNLMS had the least satisfactory results in that regard. In terms of complexity, FBNLMS was quite faster than both the other algorithms, could perform the DSI removal in less time than the coherent processing interval (CPI) and thus, was the favorable contestant for real-time processing.

The clutter removal algorithms from [64] will not be repeated in this work. The experimental part of this thesis contains the exact parameters that were used to tune the clutter removal algorithms.

5.4.2 Cross-Ambiguity Function (CAF)

After the clutter removal process, observation signal contains only the targets' reflections $s_{tar}[n]$ and noise. This enables the calculation of the cross-ambiguity function (CAF):

$$|\psi(\tau, f)| = \left| \sum_{n=0}^{C-1} s_{tar}[n]\, s_r^*[n-\tau]\, \exp\left(\frac{j\,2\pi\, f\, n}{F_s}\right) \right|, \tag{5.12}$$

where C is the number of samples of one coherent processing interval (CPI), $s_r[n]$ is the reference signal, f is the Doppler frequency and F_s is the sampling frequency; CAF is a cross-correlation of the observation signal with the reference signal with various delays τ and frequency shifts f, in order to create an amplitude-range-Doppler (ARD) map. An efficient algorithm for this procedure is described in [64].

5.4.3 Constant False Alarm Rate (CFAR) Detection

In the constant false alarm rate (CFAR) detection stage, the level of the probability of false alarm is kept constant and is given as an input. False alarms occur when an ARD surface cell has a large value, although there are no targets with the corresponding bistatic range and Doppler shift. This is often due to remaining clutter or thermal noise. The probability of detection varies according to the noise variance. The standard cell-averaging CFAR is used, described in [20]. More specifically, the number of cells for averaging is $M = 20$, with 10 on each side of the cell under test (CUT). The closest $G = 4$ cells on each side to the CUT are omitted from the averaging procedure and are called guard cells. The threshold level is set at 3db.

Chapter 6

Bistatic Tracker

This section describes the basic principles for a basic Kalman filter tracker using the bistatic measurements from the ARD surface as input and estimating the bistatic range and velocity of targets [66], [20].

6.1 Kalman Filter Theory

The Kalman filter (KF) is used to estimate the state of an evolving process $\mathbf{x}$, given a discrete set of noisy measurements.

First, there is the system evolution from time k − 1 to time k:

$$\mathbf{x}_k = \mathrm{f}(\mathbf{x}_{k-1}, \mathbf{v}_{k-1}), \tag{6.1}$$

with $\mathrm{f}(\cdot)$ the state transition model, $\mathbf{x}_{k-1}$ the previous system state and $\mathbf{v}_{k-1}$ the noise process.

Then, the measurement vector $\mathbf{z}_k$ depends on the state $\mathbf{x}_k$ according to the measurement model $\mathrm{h}(\cdot)$ as follows:

$$\mathbf{z}_k = \mathrm{h}(\mathbf{x}_k, \mathbf{w}_k), \tag{6.2}$$

where $\mathbf{w}_k$ is the measurement noise. The true system states are a combination between the state transition and the measurement model.

When both $\mathrm{f}(\mathbf{x}_{k-1}, \mathbf{v}_{k-1})$ and $\mathrm{h}(\mathbf{x}_k, \mathbf{w}_k)$ are linear functions and both $\mathbf{v}_{k-1}$ and $\mathbf{w}_k$ are additive Gaussian random variables, the Kalman filter produces the optimal *mean squared error* estimate of $\mathbf{x}_k$.

Matrix definitions at each time-step follow:

- $\mathbf{F_k}$: the state-transition model;
- $\mathbf{Q_k}$: the covariance of the process noise;
- $\mathbf{H_k}$: the observation model;

- $\mathbf{R_k}$: the covariance of the observation noise.
- Initial state – unknown, random variable with known mean (initial estimate) and covariance (initial uncertainty).

The state estimate $\mathbf{x}_k$ and the associated covariance $\mathbf{P}_k$ summarize the information from previous stages.

The state transition model $\mathbf{F}_k$ can be expressed as:

$$\mathbf{x}_k^- = \mathbf{F}_k \, \mathbf{x}_{k-1} + \mathbf{v}_{k-1}, \tag{6.3}$$

and the measurement model $\mathbf{H}_k$ as:

$$\mathbf{z}_k = \mathbf{H}_k \, \mathbf{x}_k^- + \mathbf{w}_k. \tag{6.4}$$

The process noise $\mathbf{v}_k$ and measurement noise $\mathbf{w}_k$ are described as follows:

$$\mathbf{v}_k \sim \mathbf{N}(\mathbf{0}, \mathbf{Q}_k), \tag{6.5}$$

$$\mathbf{w}_k \sim \mathbf{N}(\mathbf{0}, \mathbf{R}_k). \tag{6.6}$$

Kalman filter is a consecutive cycle between prediction and measurement updates. First, the current state is predicted by the state transition model:

$$\mathbf{x}_k^- = \mathbf{F}_k \, \mathbf{x}_{k-1}. \tag{6.7}$$

Next, the covariance matrix, which gives the uncertainty of the predicted state estimate, is estimated during the prediction stage as follows:

$$\mathbf{P}_k^- = \mathbf{F}_k \, \mathbf{P}_{k-1} \, \mathbf{F}_k^T + \mathbf{Q}_{k-1}. \tag{6.8}$$

Then, the measurement update combines the information of the measurement $\mathbf{z}_k$ of the current time step k, with the predicted estimate:

$$\mathbf{y}_k = \mathbf{z}_k - \mathbf{H}_k \, \mathbf{x}_k^-, \tag{6.9}$$

$$\mathbf{x}_k = \mathbf{x}_k^- + \mathbf{K}_k \, \mathbf{y}_k \tag{6.10}$$

$$\mathbf{P}_k = \mathbf{P}_k^- - \mathbf{K}_k \, \mathbf{H}_k \, \mathbf{P}_k^-, \tag{6.11}$$

where $\mathbf{K}_k$ is the Kalman gain and $\mathbf{y}_k$ is the measurement residual or innovation.

The Kalman gain is denoted as follows:

$$\mathbf{K}_k = \mathbf{P}_k^- \, \mathbf{H}_k^T \, \mathbf{S}_k^{-1}, \tag{6.12}$$

and the innovation covariance is given as:

$$\mathbf{S}_k = \mathbf{H}_k \, \mathbf{P}_k^- \, \mathbf{H}_k^T + \mathbf{R}_k. \tag{6.13}$$

6.2 Track Initiation

The tracker uses a standard M-out-of-N initiation logic, which states that a track is considered "preliminary" until it has been observed in M out of the last N ARD surfaces. In this case, it is confirmed. There are various alternatives in choosing the fraction M/N, affecting both the probability of detection (P_D) and false alarm (P_{FA}) [66].

6.3 Association Gate

The association gate (or validation) region is the region inside of which the measurements are considered valid association candidates to belong to a specific target [66]. Its purpose is to restrict the space where the target's measurement is considered more likely to occur. This region is defined as follows:

$$\mathbf{V}_k(\gamma) = [z_k - \hat{z}_k]^T \, \mathbf{S}_k^{-1} \, [z - \hat{z}_k] \leq \gamma, \tag{6.14}$$

and it is an ellipsoid. The gate probability is:

$$P_G \triangleq P \{ z_k \in \mathbf{V}_k(\gamma) \} \tag{6.15}$$

denoting the probability that the target's actual measurement will lie inside the ellipsoid.

Then, one could choose between the valid association candidates to find which one is the most suitable. Among them, there will be the true measurement and false alarms due to clutter residual or thermal noise. There are various alternatives on the selection and some of them will be listed below:

- Non-Bayesian association techniques

  - Nearest Neighbor Standard Filter (NNSF),
  - Strongest Neighbor Standard Filter (SNSF),

- Bayesian association techniques
  - Probabilistic Data Association Filter (PDAF).

In the Non-Bayesian association techniques, the tracking procedure is the following:

1. Validation of measurements.
2. Selection of one of the validated measurements.
3. Update the tracker using the chosen measurement.

Step 2 has two alternatives; either choosing the measurement closest to the predicted measurement (NNSF) or the strongest one (in terms of intensity) inside the validation region (SNSF). In this work, the Non Bayesian techniques were used, although PDAF or other Bayesian techniques could potentially improve the performance of the tracker.

6.4 Experimental Results

The measurement vector is given as follows:

$$\mathbf{x}_k = [r_k \ \dot{r}_k \ f_k \ \dot{f}_k]^T, \tag{6.16}$$

where r_k is the bistatic range, $\dot{r}_k$ the bistatic range rate, f_k the Doppler frequency and $\dot{f}_k$ the Doppler frequency change rate.

The state transition model is constant and is described as follows:

$$\mathbf{F}_k = \mathbf{F} = \begin{bmatrix} 1 & 0 & -\lambda\,\delta\tau & 0 \\ 0 & 0 & -\lambda & -\lambda\,\delta\tau \\ 0 & 0 & 1 & \delta\tau \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{6.17}$$

$$\mathbf{x}_k^- = \mathbf{F}\,\mathbf{x}_{k-1}, \tag{6.18}$$

where λ is the signal's wavelength and $\delta\tau$ is the update rate or the rate of new incoming measurements to the tracker. The covariance matrix is calculated as follows:

$$\mathbf{P}_k^- = \mathbf{F}\,\mathbf{P}_{k-1}\,\mathbf{F}^T + \mathbf{Q}_k. \tag{6.19}$$

The initial values of the state covariance matrix $\mathbf{P}_0$ and the process noise covariance matrix $\mathbf{Q}_k$ in the FM signal's case are listed below:

$$\mathbf{P}_0 = \begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 0.0225 & 0 & 0 \\ 0 & 0 & 0.04 & 0 \\ 0 & 0 & 0 & 0.1 \end{bmatrix}, \tag{6.20}$$

$$\mathbf{Q}_k = \mathbf{Q} = \begin{bmatrix} 3.0 & 0 & 0 & 0 \\ 0 & 0.02 & 0 & 0 \\ 0 & 0 & 0.2 & 0 \\ 0 & 0 & 0 & 0.05 \end{bmatrix}, \tag{6.21}$$

with $\mathbf{P}_0$ basic units of measurement being km and Hz and the covariance matrix $\mathbf{Q}$ kept constant in time. Also, the covariance matrix $\mathbf{R}_k$ modelling the bistatic measurement errors is a matrix kept constant in time, given as follows:

$$\mathbf{R_k} = \mathbf{R} = \begin{bmatrix} 4.0 & 0 \\ 0 & 2.0 \end{bmatrix}. \tag{6.22}$$

For the experiment, automatic dependent surveillance-broadcast (ADSB) data were used as the baseline, since they are considered much more precise. Flight SEH2CQ departing at 07: 00 UTC, in the 1st of November, 2022, from the local airport in Chania to Athens was tracked for 110 seconds between 07: 04: 58 to 07: 06: 23. The clutter removal algorithm is Least Squares (LS) with filter tap number $M = 50$, applied in Doppler shifts -2 Hz to 2 Hz around the central frequency. The CPI and tracker update rate were both set at $T_{\text{CPI}} = \delta\tau = 1$ s and the sampling frequency $F_s = 200$ kHz. The gate value was $\gamma = 16$, which corresponds to a gate probability $P_G = .9997$. Also, the association filter was chosen to be SNSF. It was observed, that due to the range sidelobes, SNSF performed better than the NSSF both in terms of accuracy and in terms of tracks lost. The initiation logic was set to be $M/N = 4/5$. The results in terms of bistatic range and Doppler shift are shown in Figs. 6.1 and 6.2.

Both the bistatic range and Doppler tracked values are relatively close to the true data. More specifically, the mean absolute error (MAE) of the bistatic range is below 800 m and below 12 Hz in the Doppler frequency. This range deviation is expected since exploiting FM signals gives a range resolution $\Delta R = c/(BW)$ ranging

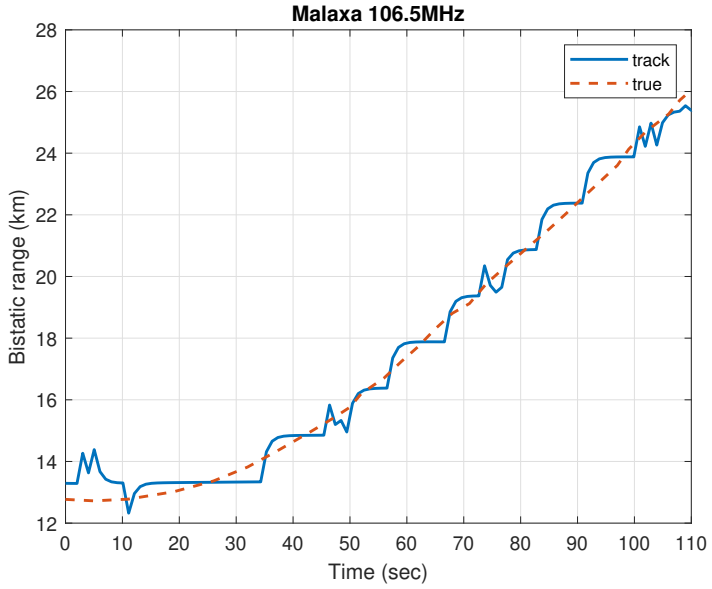


Figure 6.1: Track estimated bistatic range vs ground truth.

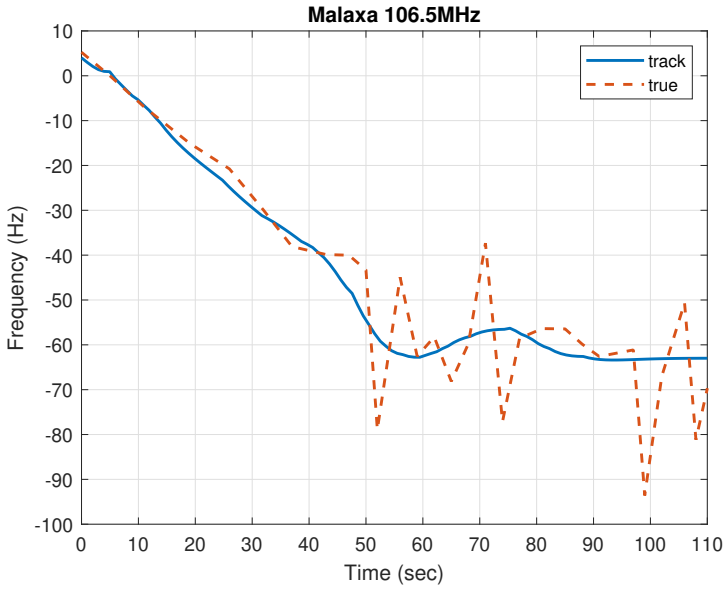


Figure 6.2: Track estimated Doppler frequency vs ground truth.

between 1500 to 3000 m, depending on the instantaneous bandwidth of the station. The narrow FM bandwidth enables large integration times (i.e. 1 s) and thus, a fine Doppler resolution (i.e. $1/T = 1$ Hz). Therefore, Doppler measurements are expected to be more precise.

Chapter 7

Cartesian 3D Tracking

In this chapter, the Cartesian 3D position and velocity tracker used will be analysed; specifically, given range-Doppler estimations from at least three ambient illuminators, the 3D state of the target will be offered; performance will be evaluated through simulation results, that correspond to a realistic scenario with one PBR station and three FM transmitters.

7.1 Localization algorithm

There are various algorithms to localize a target using multistatic radar [48], [67]. There is the direction of arrival (DOA)-based localization [46], where one has both the bistatic range and the target's azimuth. Also, there is the multilateration method in which the intersection points of three or more bistatic ellipsoids are used. The DOA-based method is considered to have low precision, due to the large wavelengths of the antennas in VHF. In our case, the multilateration method will be examined.

The Cartesian tracker needs an initialization point of the target's position and velocity. The localization algorithm used is the spherical intersection (SX) [48]. This algorithm works in a multi-transmitter and single receiver setup or vice versa. The solution is in closed form and its accuracy is heavily influenced by the geometry of the scene, as demonstrated in [48].

7.2 Nonlinear tracker

The Extended Kalman Filter (EKF) is a suboptimal state estimation algorithm for nonlinear systems. When either of the functions f(·) or h(·) is nonlinear, these functions are approximated by the evaluation of the Jacobians:

$$F_k = \frac{\partial f_k}{\partial x}\Big|_{x=x_{k-1}}, \tag{7.1}$$

$$H_k = \frac{\partial h_{k+1}}{\partial x}\Big|_{x=x_k^-}. \tag{7.2}$$

The rest of the steps are the same as in the standard Kalman filter.

The target motion model in the Cartesian coordinates is the following (subscript "c" stands for Cartesian):

$$\mathbf{x}_{c,k}^{-} = \mathbf{F}_c \, \mathbf{x}_{c,k-1} + \mathbf{u}_{c,k-1}, \tag{7.3}$$

where $\mathbf{x}_{c,k} = \begin{bmatrix} x & v_x & y & v_y & z & v_z \end{bmatrix}'$ is the state vector, $\mathbf{F}_c$ is the transition matrix and $\mathbf{u}_c$ is the process noise. The measurements for both the Cartesian position and velocity are obtained from the localization step, described in Sec. 7.1.

The bistatic measurements from the PR nodes are:

$$\mathbf{z}_{bi,k} = h_i(\mathbf{x}_{c,k}^{-}) + \mathbf{w}_{i,k}, \tag{7.4}$$

where $\mathbf{z}_{bi,k}$ is the vector of bistatic measurements (range and range rate) of the ith transmitter, $h_i(\cdot)$ is the nonlinear function connecting the Cartesian measurements with the bistatic measurements for the ith transmitter and $\mathbf{w}_{i,k}$ denotes the zero-mean Gaussian distributed measurement noise with covariance matrix:

$$\tilde{\mathbf{R}}_{ci} = E[\mathbf{w}_{i,k}\mathbf{w}_{i,k}'] = \begin{bmatrix} \sigma_R^2 & 0 \\ 0 & \sigma_V^2 \end{bmatrix}, \tag{7.5}$$

with σ_R and σ_V the standard deviation of the bistatic range and the bistatic velocity of each PR node's measurements, respectively. The nonlinear function $h_i(\cdot)$ converts the target's state vector from the Cartesian to the bistatic domain:

$$\begin{bmatrix} \mathbf{R}_i \\ \mathbf{V}_i \end{bmatrix} = h_i \left(\begin{bmatrix} x \\ v_x \\ y \\ v_y \\ z \\ v_z \end{bmatrix} \right), \tag{7.6}$$

where the equations used to do the transformation are Eqs. 5.4, 5.6 for the bistatic range and velocity, respectively. This transformation occurs during the measurement update and it uses the predicted state vector $x_{c,k}^{-}$ at time k as input.

The choice between classic Kalman filter (KF) and extended Kalman filter (EKF) is driven by the relationship of the measurements with the state vector, which is denoted by the function $h_i(\cdot)$. In case it was linear, then the classical KF would be

applied. In this case, Eqs. 5.4 and 5.6 show a highly nonlinear relation between the measurements and the state vector. In such cases, EKF is the standard approach.

The nonlinear Cartesian tracker has the same prediction steps with the bistatic tracker due to the linear motion model in both domains. The prediction step of the Cartesian tracker is listed below:

$$\mathbf{x}_{c,k}^{-} = \mathbf{F}_c \, \mathbf{x}_{c,k-1}, \tag{7.7}$$

$$\mathbf{P}_{c,k}^{-} = \mathbf{F}_c \, \mathbf{P}_{c,k-1} \, \mathbf{F}_c' + \mathbf{Q}_c, \tag{7.8}$$

where $\mathbf{P}_{c,k}^{-}$ is the predicted state's covariance matrix, $\mathbf{P}_{c,k-1}$ is the corrected state's covariance matrix of the previous time step $k-1$, and $\mathbf{Q}_c$ is the process noise covariance matrix.

Also, $h_i(\cdot)$ is linearized in the EKF by computing the Jacobian matrix:

$$\mathbf{H}_{ci,k} = \frac{\partial h_i(\mathbf{x})}{\partial \mathbf{x}}\Big|_{\mathbf{x}=\mathbf{x}_{c,k}^{-}} = \begin{bmatrix} \frac{\partial \tilde{\mathbf{R}}_i}{\partial x} & \frac{\partial \tilde{\mathbf{R}}_i}{\partial v_x} & \frac{\partial \tilde{\mathbf{R}}_i}{\partial y} & \frac{\partial \tilde{\mathbf{R}}_i}{\partial v_y} & \frac{\partial \tilde{\mathbf{R}}_i}{\partial z} & \frac{\partial \tilde{\mathbf{R}}_i}{\partial v_z} \\ \frac{\partial \tilde{\mathbf{V}}_i}{\partial x} & \frac{\partial \tilde{\mathbf{V}}_i}{\partial v_x} & \frac{\partial \tilde{\mathbf{V}}_i}{\partial y} & \frac{\partial \tilde{\mathbf{V}}_i}{\partial v_y} & \frac{\partial \tilde{\mathbf{V}}_i}{\partial z} & \frac{\partial \tilde{\mathbf{V}}_i}{\partial v_z} \end{bmatrix}, \tag{7.9}$$

where the partial derivatives of the function $h_i(\cdot)$ with respect to the state prediction vector $x_{c,k}^{-}$ are calculated, using the Eqs. 5.4, 5.6.

7.2.1 Updating scheme

For the measurement update steps there are two alternatives: the parallel and the sequential approach. The parallel updating scheme can be inconvenient, due to the fact that sets of measurements are tested each time in the validation gate. Therefore, it could be a complicated task, when multiple targets are present, due to the amount of tests that must be performed. This is not a problem in the sequential approach, where each transmitter-receiver pair is treated individually.

The state estimate and its covariance matrix are set equal to the temporary variables:

$$\tilde{\mathbf{x}}_{c0,k} = \tilde{\mathbf{x}}_{c,k}, \tag{7.10}$$

$$\mathbf{P}_{c0,k} = \mathbf{P}_{c,k}, \tag{7.11}$$

and the update steps are performed for each of the N TXs, separately, as follows:

for $i = 1, \ldots, N$

$$\mathbf{S}_{ci,k} = \mathbf{H}_{ci,k}\mathbf{P}^{-}_{c(i-1),k}\mathbf{H}'_{ci,k} + \mathbf{R}_{ci}, \tag{7.12}$$

$$\mathbf{K}_{ci,k} = \mathbf{P}^{-}_{c(i-1),k}\mathbf{H}'_{ci,k}\mathbf{S}^{-1}_{c_i,k}, \tag{7.13}$$

$$\tilde{\mathbf{x}}_{ci,k} = \tilde{\mathbf{x}}^{-}_{c(i-1),k} + \mathbf{K}_{ci,k}\mathbf{v}_{ci,k}, \tag{7.14}$$

$$\mathbf{P}_{ci,k} = \mathbf{P}^{-}_{c(i-1),k} - \mathbf{K}_{c,k}\mathbf{H}_{ci,k}\mathbf{P}^{-}_{c(i-1),k}, \tag{7.15}$$

end

The bistatic measurements that are valid candidates for updating the state are tested separately for each transmitter-receiver pair, in contrast to the parallel scheme, as follows:

$$\mathbf{v}'_{ci,k}\,\mathbf{S}^{-1}_{c_i,k}\,\mathbf{v}_{ci,k} \leq \gamma, \tag{7.16}$$

with $\mathbf{v}_{ci,k}$ the innovation of the ith transmitter at time k and $\mathbf{S}_{c_i,k}$ a 2×2 innovation covariance matrix corresponding to transmitter i. Also, because all the bistatic measurements are not always available (which is the realistic case since $P_D < 1$), the sequential approach can update a track only with a subset of the transmitter-receiver pairs.

7.3 Two-stage target tracker

A two-stage tracker is presented in Fig. 7.1. From each transmitter-receiver pair an individual ARD map is generated from the CFAR detector, presented in 5.4.3. The Cartesian tracker needs an initialization point to start a Cartesian track. This is offered from the localization algorithm, discussed in 7.1. In order to avoid significant computational overhead due to false alarms, the localization process is performed with tracks produced by bistatic trackers, such as the one presented in Chapter 6. Then, the Cartesian tracker updates the targets' 3D state using the ARD maps. Any unassigned detections from the bistatic plots are used from the bistatic trackers, to create new target tracks.

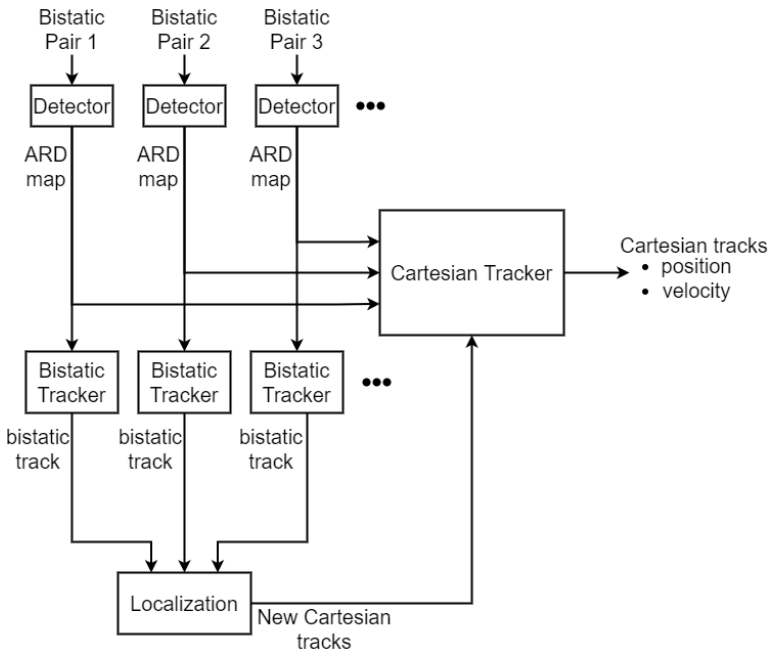


Figure 7.1: Overview of the two-stage tracker.

7.4 Simulations

According to [67], the performance of the sequential and parallel schemes is similar. Also, the sequential approach is more versatile and, therefore, it was preferred.

The two-stage tracker presented above was tested through simulations in a scenario with one receiver and three spatially separated transmitters. The target's trajectory was created using the motion model in Eq. 7.3, with $\sigma_{xy} = 1$ and $\sigma_z = 0.1$. The target's initial position is at $[10, 30, 10]$ km. The transmitters' locations are listed in Table 7.1.

Transmitter	x (km)	y (km)	z (km)
1	42	40	0.6
2	-20	0	0.3
3	10	-40	0.5

Table 7.1: Locations of the TXs in relation to the RX placed at $[0, 0, 0]$.

The first step includes the formation of bistatic tracks from the measurements. The measurements where created by adding Gaussian noise with zero mean and standard deviation $\sigma_R = 500$ m in bistatic range and $\sigma_V = 1$ m/s in bistatic velocity with $P_D = 0.75$. These values of error are expected for a narrowband FM signal. Fig. 7.2 demonstrates the noisy measurements obtained (blue dots), the bistatic track formed

(red line) and the true bistatic range value (yellow dashed line). It is clear from the figure, that although the measurements are noisy, the bistatic track formed is close to the truth. Therefore, it is shown that the Cartesian tracker increases the accuracy of the measurements compared to the ground truth. Due to the fine Doppler resolution, which leads to accurate Doppler measurements, the improvement obtained from the tracker in terms of bistatic velocity is not significant, as demonstrated in 7.3.

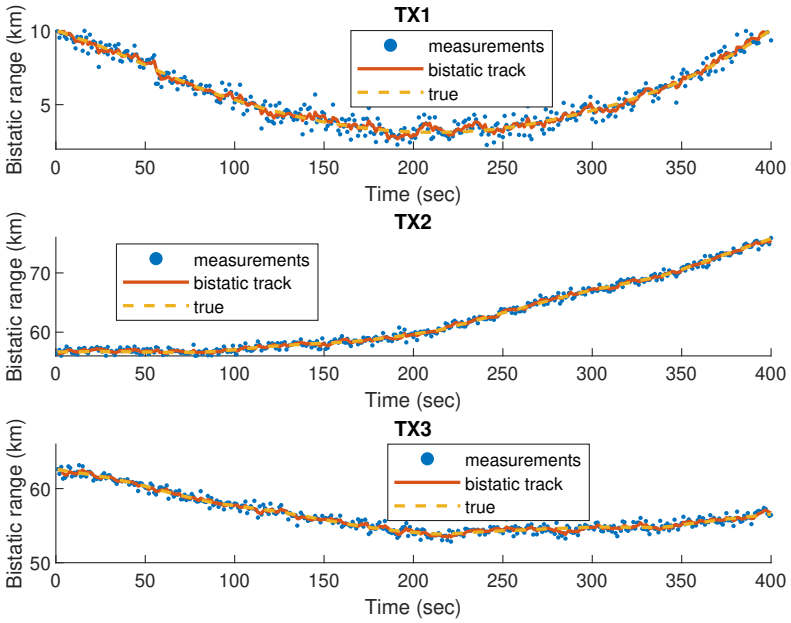


Figure 7.2: Bistatic Range (km) corresponding to noisy measurements, the tracker output and the ground truth.

In order to be more specific, the absolute error between each track state's bistatic range and the true bistatic range is shown in Fig. 7.4, where the measurements' error (blue line) is constantly significantly higher than the track's error (red line). The track error is kept mostly below 500 m, while the measurement's error is mostly between 500 and 1000 m.

Then, the target's tracked state, including 3D position and velocity, is shown in Figs. 7.5, 7.6. In Fig. 7.5, the true position of the target in the 3D axis is depicted (red line), along with the tracked values (blue dashed line). It is shown, that the tracker needs more iterations to converge on the z axis. Also, even after the convergence there are some ripples. This is in contrast to the X and Y axes, where the convergence is almost instant. The reason is the scene geometry. Although, in the x and y-axes the transmitters are spread kilometres apart, generating a more diverse scene, in the

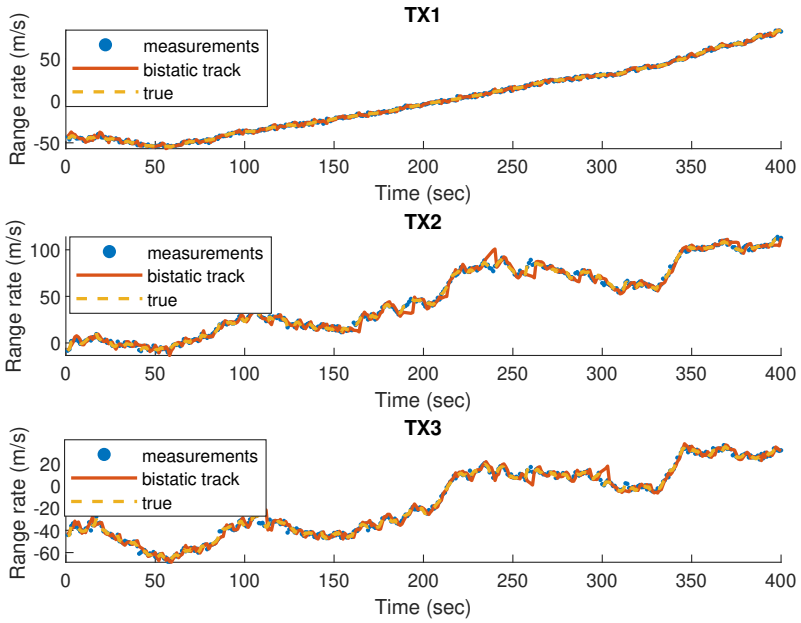


Figure 7.3: Bistatic range rate (m/s) of noisy measurements, tracked value and the ground truth.

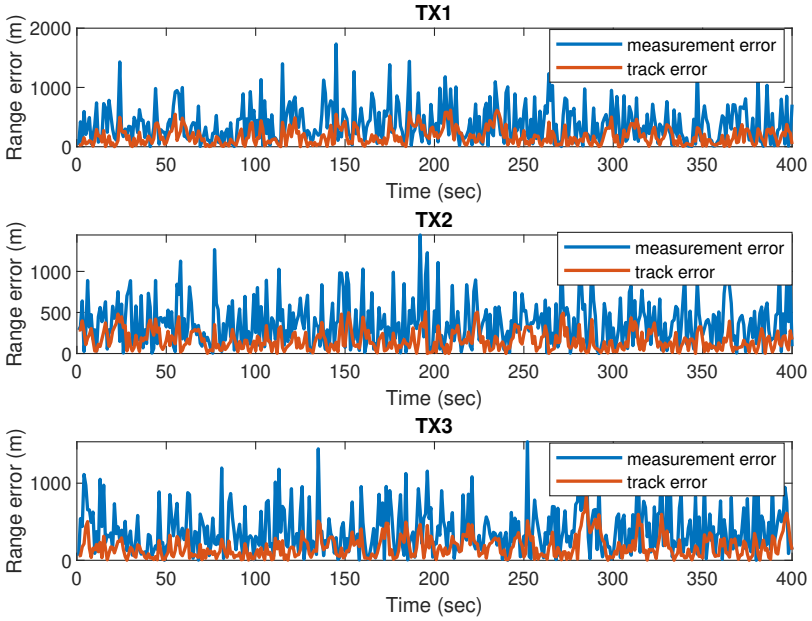


Figure 7.4: Absolute error of the noisy measurements and the tracked bistatic range from the ground truth.

z-axis this is not possible. Also, the true speed (m/s) of the plane in each of the 3 axes is depicted in Fig. 7.6, where again the z-axis is the slowest to converge.

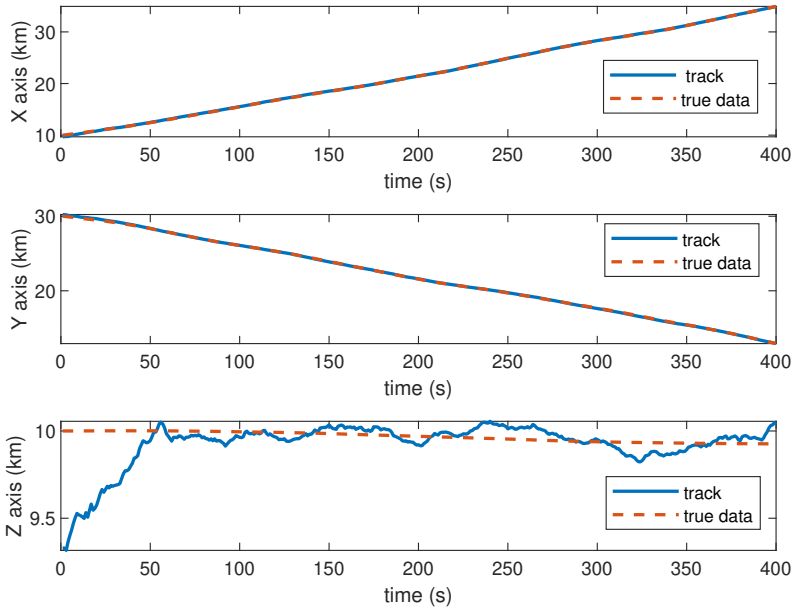


Figure 7.5: Cartesian tracker's position output vs ground truth.

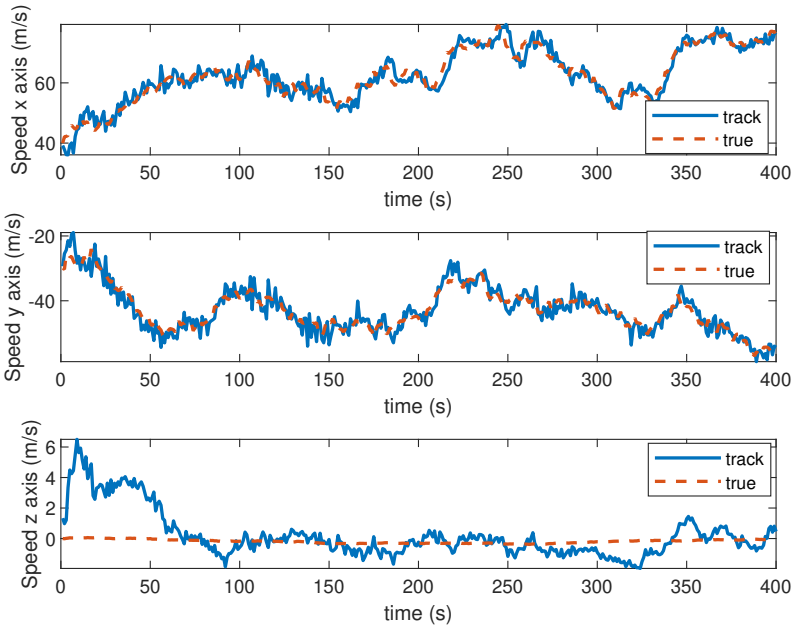


Figure 7.6: Cartesian tracker's velocity output vs ground truth.

Next, the absolute error of the plane's position is shown in Fig. 7.7. The tracker converges after approximately 50 iterations. Absolute error is kept below 100m, in all three directions.

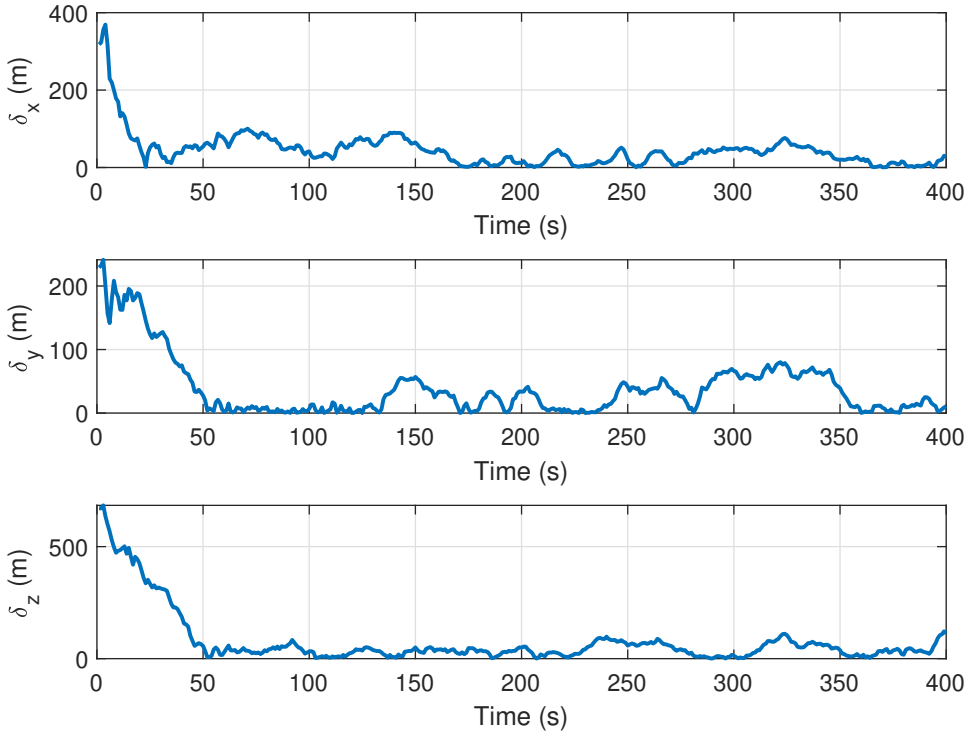


Figure 7.7: Cartesian tracker's error in range.

Chapter 8

Conclusion

It was shown that it is possible to find the optimal RIS element configuration with complexity of $\mathcal{O}(M \log M)$, offering theory and results for large number M of RIS elements, in the order of thousands; in the latter case, complexity K^M of exhaustive search is prohibitive for any similar analysis. Comparison with prior art configuration also reveals the benefits of the proposed technique. It was also found that the passive nature of RIS, i.e., lack of amplification, limits the benefits, even for extended number of RIS elements. A wireless and batteryless testbed, designed with RFID tags was also demonstrated, pointing to the necessary modifications required, in order to wirelessly control the RFID tag/RIS elements.[1] Future work could exploit findings of this work, offering a specialized protocol for more efficient wireless and batteryless RIS, with RFID and backscatter radio technology.

For the passive radar, a Cartesian tracker comprising of two stages has been presented. The simulations and the experimental results validated its performance. Initially, the raw measurements from each of the three transmitters are gathered and the corresponding bistatic tracks are formed, using the tracker of Ch. 6. This step reduces significantly the amount of false alarms that will be given as input to the next steps, thus, reducing the overall complexity of the system. In addition, the bistatic state estimates are more accurate than the raw measurements and lead to better performance of the following stages.

Next, once the bistatic tracks from all the transmitter-receiver pairs have been created, an initial position and velocity estimate is created using the localization algorithm SX. Finally, the initial point is given as input to the Cartesian tracker, which follows the 3D state of the target using a nonlinear EKF filter. Simulation results showed that by adding noise with standard deviation 500 m in range and 1 m/s in velocity, which are typical values for FM stations, a tracking accuracy below 100 m in all directions can be achieved. As future work, this experimental testbed could be expanded by using more transmitters or by adding low-cost PBR stations, without altering the tracking algorithms presented, which are fully scalable.

[1] Relevant results can be found in [68], [69]

Bibliography

[1] V. Arun and H. Balakrishnan, "RFocus: Beamforming Using Thousands of Passive Antennas," in *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*, Santa Clara, CA, Feb. 2020, pp. 1047–1061.

[2] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. D. Renzo, and M. Debbah, "Holographic MIMO Surfaces for 6G Wireless Networks: Opportunities, Challenges, and Trends," *IEEE Trans. Wireless Commun.*, vol. 27, no. 5, pp. 118–125, Oct. 2020.

[3] E. Björnson, Ö. Özdogan, and E. G. Larsson, "Reconfigurable Intelligent Surfaces: Three Myths and Two Critical Questions," *IEEE Commun. Mag.*, vol. 58, no. 12, pp. 90–96, Dec. 2020.

[4] J. Kimionis, A. Bletsas, and J. N. Sahalos, "Bistatic backscatter radio for tag read-range extension," in *Proc. IEEE Int. Conf. on RFID-Technologies and Applications (RFID-TA)*, Nice, France, Nov. 2012.

[5] ——, "Bistatic backscatter radio for power-limited sensor networks," in *Proc. IEEE Global Commun. Conf. (Globecom)*, Atlanta, GA, Dec. 2013, pp. 353–358.

[6] ——, "Increased Range Bistatic Scatter Radio," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1091–1104, Mar. 2014.

[7] P. N. Alevizos, K. Tountas, and A. Bletsas, "Multistatic scatter radio sensor networks for extended coverage," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4522–4535, Jul. 2018.

[8] M. Ouroutzoglou, G. Vougioukas, G. N. Karystinos, and A. Bletsas, "Multistatic noncoherent linear complexity Miller sequence detection for Gen2 RFID/IoT," *IEEE Trans. Wireless Commun.*, vol. 20, no. 12, pp. 8067–8080, Dec. 2021.

[9] G. Vannucci, A. Bletsas, and D. Leigh, "A software-defined radio system for backscatter sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2170–2179, Jun. 2008.

[10] E. Kampianakis, J. Kimionis, K. Tountas, C. Konstantopoulos, E. Koutroulis, and A. Bletsas, "Wireless environmental sensor networking with analog scatter radio & timer principles," *IEEE Sensors J.*, vol. 14, no. 10, pp. 3365—3376, Oct. 2014.

[11] N. Fasarakis-Hilliard, P. N. Alevizos, and A. Bletsas, "Coherent detection and channel coding for bistatic scatter radio sensor networking," *IEEE Trans. Commun.*, vol. 63, pp. 1798–1810, May 2015.

[12] C. Konstantopoulos, E. Koutroulis, N. Mitianoudis, and A. Bletsas, "Converting a plant to a battery and wireless sensor with scatter radio and ultra-low cost," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 2, pp. 388–398, Feb. 2016.

[13] S. N. Daskalakis, S. D. Assimonis, E. Kampianakis, and A. Bletsas, "Soil moisture scatter radio networking with low power," *IEEE Trans. Microwave Theory Tech.*, vol. 64, no. 7, pp. 2338–2346, Jul. 2016.

[14] P. N. Alevizos, A. Bletsas, and G. N. Karystinos, "Noncoherent short packet detection and decoding for scatter radio sensor networking," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2128–2140, May 2017.

[15] G. Vougioukas, A. Dimitriou, A. Bletsas, and J. Sahalos, "Practical energy harvesting for batteryless ambient backscatter sensors," *Electronics*, vol. 7, no. 6, p. 95, Jun. 2018.

[16] G. Vougioukas and A. Bletsas, "Switching frequency techniques for universal ambient backscatter networking," *IEEE J. Select. Areas Commun.*, vol. 37, no. 2, pp. 464–477, Feb. 2019.

[17] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," in *Proc. ACM SIGCOMM*, Hong Kong, China, 2013, pp. 39–50.

[18] A. Bletsas, P. N. Alevizos, and G. Vougioukas, "The art of signal processing in backscatter radio for μW (or less) internet of things: Intelligent signal processing and backscatter radio enabling batteryless connectivity," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 28–40, Sep. 2018.

[19] N. J. Willis, *Bistatic Radar*. Scitech Publising Inc., 2005.

[20] P. E. Howland, D. Maksimiuk, and G. Reitsma, "FM radio based bistatic radar," *IEE proceedings-radar, sonar and navigation*, vol. 152, no. 3, pp. 107–115, 2005.

[21] R. Saini and M. Cherniakov, "DTV signal ambiguity function analysis for radar application," *IEE Proceedings -Radar, Sonar and Navigation* , vol. 152, pp. 133 – 142, 07 2005.

[22] M. Malanowski, K. Borowiec, S. Rzewuski, and K. Kulpa, "Detection of supersonic rockets using passive bistatic radar," *IEEE Aerospace and Electronic Systems Magazine*, vol. 33, no. 1, pp. 24–33, 2018.

[23] M. Contu, A. De Luca, S. Hristov, L. Daniel, A. Stove, M. Gashinova, M. Cherniakov, D. Pastina, P. Lombardo, A. Baruzzi, and D. Cristallini, "Passive multifrequency forward-scatter radar measurements of airborne targets using broadcasting signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 3, pp. 1067–1087, 2017.

[24] H. Griffiths and C. Baker, "Passive coherent location radar systems. part 1: Performance prediction," *Radar, Sonar and Navigation, IEE Proceedings* -, vol. 152, pp. 153 – 159, 07 2005.

[25] W. C. Barott, "Coherent Backscatter Communications Using Ambient Transmitters and Passive Radar Processing," in *2014 National Wireless Research Collaboration Symposium*, 2014, pp. 15–20.

[26] E. Björnson and L. Sanguinetti, "Power Scaling Laws and Near-Field Behaviors of Massive MIMO and Intelligent Reflecting Surfaces," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1306–1324, Sep. 2020.

[27] F. H. Danufane, M. D. Renzo, J. de Rosny, and S. Tretyakov, "On the Path-Loss of Reconfigurable Intelligent Surfaces: An Approach Based on Green's Theorem Applied to Vector Fields," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5573–5592, Aug. 2021.

[28] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[29] J. Lyu and R. Zhang, "Spatial throughput characterization for intelligent reflecting surface aided multiuser system," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 834–838, Jun. 2020.

[30] M. Di Renzo, F. Habibi Danufane, X. Xi, J. de Rosny, and S. Tretyakov, "Analytical modeling of the path-loss for reconfigurable intelligent surfaces – anomalous mirror or scatterer ?" in *Proc. IEEE Workshop on Signal Process. Advances in Wireless Commun. (SPAWC)*, May 2020, pp. 1–5.

[31] W. Tang, M. Z. Chen, X. Chen, J. Y. Dai, Y. Han, M. Di Renzo, Y. Zeng, S. Jin, Q. Cheng, and T. J. Cui, "Wireless communications with reconfigurable intelligent surface: Path loss modeling and experimental measurement," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 421–439, Jan. 2021.

[32] M. Di Renzo, A. Zappone, M. Debbah, M.-S. Alouini, C. Yuen, J. de Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Select. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.

[33] M. A. Kishk and M. S. Alouini, "Exploiting randomly located blockages for large-scale deployment of intelligent surfaces," *IEEE J. Select. Areas Commun.*, vol. 39, no. 4, pp. 1043–1056, Apr. 2021.

[34] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-lin, and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sep. 2015.

[35] A. S. d. Sena, D. Carrillo, F. Fang, P. H. J. Nardelli, D. B. d. Costa, U. S. Dias, Z. Ding, C. B. Papadias, and W. Saad, "What role do intelligent reflecting surfaces play in multi-antenna non-orthogonal multiple access?" *IEEE Trans. Wireless Commun.*, vol. 27, no. 5, pp. 24–31, Oct. 2020.

[36] C. Zhang, W. Yi, and Y. Liu, "Reconfigurable intelligent surfaces aided multi-cell NOMA networks: A stochastic geometry model," Aug. 2020. [Online]. Available: http://arxiv.org/abs/2008.08457

[37] Y. Cheng, K. H. Li, Y. Liu, K. C. Teh, and H. Vincent Poor, "Downlink and uplink intelligent reflecting surface aided networks: NOMA and OMA," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3988–4000, Jun. 2021.

[38] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162–169, Sep. 2018.

[39] C. Liaskos, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "Using any surface to realize a new paradigm for wireless communications," *Commun. ACM*, vol. 61, no. 11, pp. 30–33, Oct. 2018.

[40] S. Abadal, C. Liaskos, A. Tsioliaridou, S. Ioannidis, A. Pitsillides, J. Solé-Pareta, E. Alarcón, and A. Cabellos-Aparicio, "Computing and communications for the software-defined metamaterial paradigm: A context analysis," *IEEE Access*, vol. 5, pp. 6225–6235, Apr. 2017.

[41] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "Realizing wireless communication through software-defined hypersurface environments," in *IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Jun. 2018, pp. 14–15.

[42] C. K. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. F. Akyildiz, "A novel communication paradigm for high capacity and security via programmable indoor wireless environments in next generation wireless systems," *Ad Hoc Networks*, vol. 87, pp. 1–16, 2019.

[43] Z. Li, Y. Xie, L. Shangguan, R. I. Zelaya, J. Gummeson, W. Hu, and K. Jamieson, "Towards Programming the Radio Environment with Large Arrays of Inexpensive Antennas," in *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, Boston, MA, Feb. 2019, pp. 285–300.

[44] L. Dai, B. Wang, M. Wang, X. Yang, J. Tan, S. Bi, S. Xu, F. Yang, Z. Chen, M. D. Renzo, and L. Hanzo, "Reconfigurable Intelligent Surface-Based Wireless Communications: Antenna Design, Prototyping, and Experimental Results," *IEEE Access*, vol. 8, pp. 45 913–45 923, Mar. 2020.

[45] W. Tang, J. Y. Dai, M. Z. Chen, K.-K. Wong, X. Li, X. Zhao, S. Jin, Q. Cheng, and T. J. Cui, "MIMO transmission through reconfigurable intelligent surface: System design, analysis, and implementation," *IEEE Trans. Commun.*, vol. 38, no. 11, pp. 2683–2699, Nov. 2020.

[46] H. Huang, "Array-Based Localization in DTV Passive Radar," Ph.D. dissertation, School of ECE, The Ohio State University, 2019, advisor: Graeme Smith.

[47] Q. He and R. S. Blum, "The Significant Gains From Optimally Processed Multiple Signals of Opportunity and Multiple Receive Stations in Passive Radar," *IEEE Signal Processing Letters*, vol. 21, no. 2, pp. 180–184, 2014.

[48] M. Malanowski and K. Kulpa, "Two methods for target localization in multistatic passive radar," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 48, pp. 572–580, Jan. 2012.

[49] A. Noroozi and M. A. Sebt, "Target Localization from Bistatic Range Measurements in Multi-Transmitter Multi-Receiver Passive Radar," *IEEE Signal Processing Letters*, vol. 22, no. 12, pp. 2445–2449, 2015.

[50] M. Klein and N. Millet, "Multireceiver passive radar tracking," *IEEE Aerospace and Electronic Systems Magazine*, vol. 27, no. 10, pp. 26–36, 2012.

[51] F. Colone, C. Bongioanni, and P. Lombardo, "Multifrequency integration in FM radio-based passive bistatic radar. Part I: Target detection," *IEEE Aerospace and Electronic Systems Magazine*, vol. 28, no. 4, pp. 28–39, 2013.

[52] M. Malanowski, K. Borowiec, S. Rzewuski, and K. Kulpa, "Detection of supersonic rockets using passive bistatic radar," *IEEE Aerospace and Electronic Systems Magazine*, vol. 33, no. 1, pp. 24–33, 2018.

[53] M. Manning. [Online]. Available: https://dopplerfish.com/passive-radar/

[54] P. Tamas. [Online]. Available: https://github.com/petotamas/APRiL

[55] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.

[56] A. Bletsas, A. G. Dimitriou, and J. N. Sahalos, "Improving Backscatter Radio Tag Efficiency," *IEEE Trans. Microwave Theory Tech.*, vol. 58, no. 6, pp. 1502–1509, Jun. 2010.

[57] P. N. Alevizos, Y. Fountzoulas, G. N. Karystinos, and A. Bletsas, "Log-Linear-Complexity GLRT-Optimal Noncoherent Sequence Detection for Orthogonal and RFID-Oriented Modulations," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1600–1612, Apr. 2016.

[58] Y. Zhang, K. Shen, S. Ren, X. Li, X. Chen, and Z.-Q. Luo, "Configuring intelligent reflecting surface with performance guarantees: Optimal beamforming," *IEEE J. Sel. Top. Signal Process.*, vol. 16, no. 5, pp. 967–979, Aug. 2022.

[59] G. Vougioukas, A. Bletsas, and J. N. Sahalos, "Instantaneous, Zero-Feedback Fading Mitigation with Simple Backscatter Radio Tags," *IEEE J. Radio Freq. Identif.*, Oct. 2020, early access.

[60] N. Kargas, F. Mavromatis, and A. Bletsas, "Fully-Coherent Reader With Commodity SDR for Gen2 FM0 and Computational RFID," *IEEE Wireless Commun. Lett.*, vol. 4, no. 6, pp. 617–620, Dec. 2015.

[61] Alien Technology LLC, "HIGGS-EC High Sensitivity RFID IC Datasheet," https://www.alientechnology.com/download/higgs-ec-files/?wpdmdl=7564&ind=QUxDLTM4MCBIaWdncy1FQyAyMDIwLTAyLTIxLnBkZg.

[62] Q. Wu and R. Zhang, "Intelligent Reflecting Surface Enhanced Wireless Network: Joint Active and Passive Beamforming Design," in *Proc. IEEE Global Commun. Conf. (Globecom)*, Dec. 2018, pp. 1–6.

[63] ——, "Beamforming Optimization for Intelligent Reflecting Surface with Discrete Phase Shifts," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Mar. 2019, pp. 7830–7833.

[64] I. Vardakis, "Passive radar with ambient illuminators and low-cost software-defined radios," Diploma thesis available in: https://dias.library.tuc.gr/view/86359?locale=en, School of ECE, Technical University of Crete, Chania, Greece, Jul. 2020, Supervisor A. Bletsas.

[65] K6STI, "Small Five-Element Yagi." [Online]. Available: http://ham-radio.com/k6sti/five.htm

[66] Y. Bar-Shalom and X.-R. Li, *Multitarget-multisensor tracking: principles and techniques*. YBs Storrs, CT, 1995, vol. 19.

[67] M. Malanowski, *Signal Processing for Passive Bistatic Radar*. ARTECH HOUSE, 2019.

[68] I. Vardakis, G. Kotridis, S. Peppas, K. Skyvalakis, G. Vougioukas, and A. Bletsas, "Intelligently Wireless Batteryless RF-Powered Reconfigurable Surface," in *Proc. IEEE Global Commun. Conf. (Globecom)*, 2021, pp. 1–6.

[69] ——, "Intelligently Wireless Batteryless RF-Powered Reconfigurable Surface: Theory, Implementation & Limitations," *IEEE Trans. Wireless Commun.*, accepted.